ANTlabs
Connectivity Made Easy

INNGATE 3

ADMINISTRATOR'S MANUAL

DOCUMENT RELEASE 1.01

Powered by
ezxcess GATEWAY

Incorporating
truconnect TECHNOLOGY

This manual provides an in-depth coverage of the setup, configuration and administration of an InnGate 3 and is intended for system and network administrators who will be performing these tasks.

Copyright © 2002 - 2009 Advanced Network Technology Laboratories Pte Ltd.
All rights reserved.

TRADEMARKS AND ACKNOWLEDGEMENTS

The following trademarks and acknowledgments apply to the following: The InnGate system and Tru'Connect™ technology are products and technologies of Advanced Network Technology Laboratories Pte Ltd, (ANT*labs*). Windows and Microsoft are registered trademarks of Microsoft Corporation. Solaris is a registered trademark of Sun Microsystems. All other products mentioned in this manual are trademarks of their respective owners.

DISCLAIMER

No part of this manual may be copied, distributed, transmitted, transcribed, stored in a retrieval system or translated into any human or computer language, in any form or by any means, electronic or otherwise, without the express written permission of ANT*labs*.

The software and accompanying written materials (including instructions for use and this document) are provided "as is" without warranty of any kind.

ANT*labs* does not warrant, guarantee or make any representations regarding the use, or the results of the use, of the software or written materials in terms of correctness, accuracy, reliability, trend or otherwise. ANT*labs* reserves the right to make changes without further notice to any products described herein to improve reliability, function or design. This documentation is copyrighted and may not be altered without written consent from ANT*labs*.

ANT*labs* reserves the right to prosecute companies or individuals who make, distribute or use illegal copies of this software system and its accompanying documentation.

Release Date: 10 July 2009
Document Reference No: IG3-ADM

CONTENTS

Chapter 1 9
GETTING STARTED 9
1.1 Overview 9
1.1.1 Hardware 10
1.1.2 Network Operation 11
1.2 Recommended Setting 12
1.3 System Setup 12
1.3.1 Accessing the Web-based Admin GUI 13
1.3.2 Configuring the WAN Interface 15
1.3.3 Configuring the Domain Name Server 17
1.3.4 Configuring the Web Proxy 18
1.3.5 Creating a Plan 20
1.3.6 Firewall Rules 22
1.3.7 Creating a Location 24
1.3.8 Creating VLANs 32
1.3.9 Importing and Exporting VLAN Definitions 34
1.4 Network Installation 35
1.4.1 VLAN-enabled Networks 36
1.5 Testing the Configuration 36
Chapter 2 38
Authentication 38
2.1 Overview 38
2.2 Local Accounts 38
2.2.1 Local Accounts Maintenance 40
2.3 PMS 40
2.4 Account Printers 43
2.5 Credit Card 47
2.6 MAC Filter 47
2.7 Global Settings 48
Chapter 3 50
LAN NETWORK SETTINGS 50
3.1 Overview 50
3.2 DHCP Setup 51
3.2.1 Configuring DHCP Server Mode 51
3.2.1.1 Setting up the Default Scope 53
3.2.1.2 Setting up the User Provision Routed Scope 55
3.2.2 Configuring DHCP Relay Mode 60
3.2.2.1 Relay Agent Mappings 61
3.3 Routed Network Setup 62
3.4 Walled Garden Setup 64
3.4.1 Define HTTP URLs 65
3.4.2 Define HTTPS Domains 67
3.4.3 Define IP Addresses 69
3.5 Network Devices Setup 71
3.5.1 Port Binding 72

3.6 Device Detection Setup 75
3.7 ARP Setup 76
Chapter 4 78
WAN NETWORK SETTINGS 78
4.1 Overview 78
4.2 WAN Setup 78
4.2.1 Defining a Static Route 78
Chapter 5 80
NETWORK SERVICES SETTINGS 80
5.1 Overview 80
5.2 Web Server 80
5.3 Web Proxy 81
5.4 Email Server 81
5.5 Remote Access 84
5.5.1 Accessing the InnGate via Telnet and FTP 86
Chapter 6 87
SYSTEM MAINTENANCE AND DIAGNOSTICS 87
6.1 Overview 87
6.2 Local Accounts Maintenance 87
6.3 Reports Maintenance 88
6.4 PMS Diagnostics 90
Chapter 7 92
SYSTEM MONITORING AND REPORTING 92
7.1 Overview 92
7.2 Monitors 92
7.2.1 Status Monitor 92
7.2.2 Device Monitor 94
7.2.3 Session Monitor 96
7.2.4 Account Monitor 97
7.2.5 Cookies Monitor 99
7.2.6 Email Monitor 100
7.3 Logs 101
7.3.1 Device Logs 101
7.3.2 Session Logs 102
7.3.3 PMS Logs 103
7.3.4 Account Printer Logs 105
7.3.5 Credit Card Logs 106
7.4 Maintenance 106
Chapter 8 107
SYSTEM ADMINISTRATION 107
8.1 Overview 107
8.2 Setting up Administrator Accounts 107
8.2.1 Creating an Administrator Group 108
8.2.2 Defining Admin Group Permissions 109
8.2.3 Creating an Administrator Account 110
8.2.4 Viewing Audit Log 112
8.2.5 Assigning Admin Access 112
8.2.6 Viewing Sessions 113

8.3 Powering up and shutting down the system 113
8.4 System Configuration Backup or Restore 114
8.5 Applying System Patches 115
8.6 Setting the Date and Time 116
8.7 Syslog Configuration 117
8.8 SNMP Setup 118
8.8.1 Traps Generated 120
8.8.2 Supported MIBs 124
8.9 View API Information 124
8.9.1 HTTP Setting 125
8.9.2 Browser Setting 126
8.10 High Availability 128
8.11 View License Information 128
8.12 Console Access via Serial Connection 128
8.13 Securing the System for Deployment 129
8.13.1 Securing Access to the Admin GUI 129
8.13.2 Change the Default Admin User Account 130
8.13.3 Change the FTP Account Password 131
8.13.4 Change the Telnet and Console Password 131
Chapter 9 133
HIGH AVAILABILITY (E-Series) 133
9.1 Overview 133
9.2 Network Configuration 133
9.3 System Configuration 134
9.3.1 HA Identifier 136
9.4 HA Leader Election 137
9.5 HA Failover Behavior 137
9.6 HA Synchronization 138
9.6.1 Manual Synchronization 139
Chapter 10 141
HIGH AVAILABILITY (M-Series) 141
10.1 Overview 141
10.2 Network Configuration 141
10.3 System Configuration 142
10.4 Billing Configuration 144
10.5 Failover Behavior 145
Chapter 11 146
System Save & Restoration 146
11.1 Overview 146
11.2 Save Snapshot 146
11.3 Restore Firmware 147
11.4 Restore Snapshot 149
Appendix A 151
REDIRECT LOG 151
Appendix B 154
PERL REGULAR EXPRESSIONS 154
Appendix C 155
CSV FILE RESTRICTIONS 155

Appendix D 156
UPLOADING CUSTOM WEBPAGES 156
Appendix E 157
CUSTOM SSL LOGIN PAGES 157
Appendix F 161
ERROR PAGES 161
Appendix G 163
CREDIT CARD 163

AUDIENCE

This manual is intended for administrators who will be responsible for the installation and configuration of the InnGate 3.

This manual will explain how first-time installation and configuration should be done as well as the tasks involved in performing regular maintenance and configuration.

Administrators are expected to have a good working knowledge of networks and TCP/IP. Knowledge of the operating environment and characteristics of the systems used in the deployed networks are also useful. Basic knowledge of HTML and HTTP will also allow the administrator to customize the user-facing web pages.

RELATED DOCUMENTATION

You may refer to the ANT*labs* homepage at **http://www.antlabs.com/** for other related materials and documents released by ANT*labs*.

FEEDBACK AND COMMENTS

ANT*labs* welcomes all comments and suggestions on the quality and usefulness of this document. Our users' feedback is an important component of the information used for improvement of this document.

Please include in your feedback:

- Name
- Title
- Company
- Department
- E-Mail
- Postal Address
- Telephone Number
- Document Title & Release No
- Document Reference No.
- Comments/Feedback

Also, please include the chapter, section and/or page number when referring to specific portions of the document.

Send your comments via email to **documentation@antlabs.com**

Chapter 1

GETTING STARTED

1.1 Overview

This chapter will illustrate a simple network deployment of the InnGate 3 involving the following 3 steps:

1. **System Setup** – Configuring the InnGate to operate in the network.

2. **Network Installation** – Connecting the InnGate to the network.

3. **Testing the Configuration** – Ensuring that the InnGate operates as expected.

Figure 1-1 shows a simple network setup which will be used to illustrate the deployment steps in this chapter.

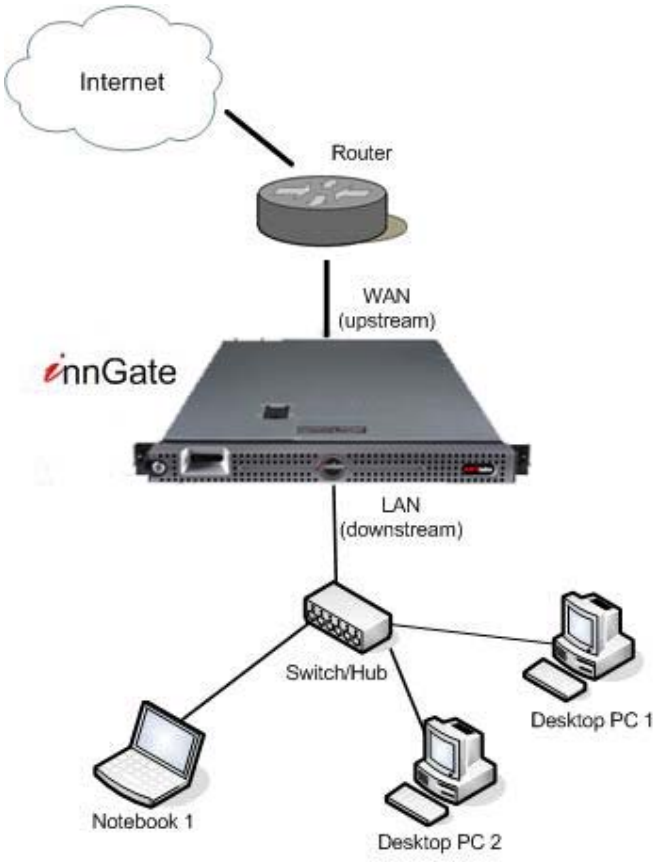


Figure 1-1 Example Network Diagram

Although your own network will likely differ from this, the general principles for installing and configuring the InnGate are still applicable.

The setup covered in this chapter is suitable for quick demonstrations and small-scale setups. Later chapters will cover details for more complex deployment scenarios.

1.1.1 Hardware

Front Panel

Back Panel

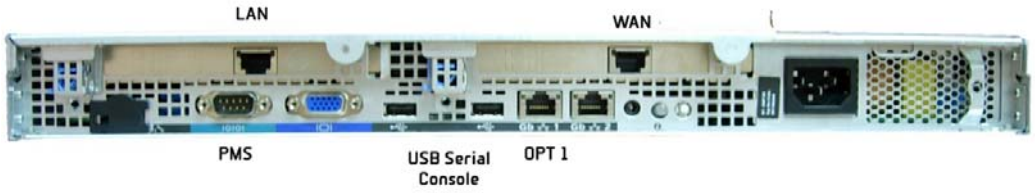


Figure 1-2 InnGate E Series Front & Back Panels

Front Panel

Back Panel

Figure 1-3 InnGate M Series Front & Back Panels

Some of the switches and connectors shown in Figure 1-2 and Figure 1-3 are described here:

1. **USB Serial Console** – The left USB port allows direct console access to the InnGate. Use the provided USB-to-serial converter to connect a PC with a terminal program to access the console (see Section 8.12).

2. **Serial Console** – The M-series serial console allows direct console access to the InnGate.

3. **LAN** – All clients to be managed by the InnGate are placed on the network which is connected to this port.

4. **WAN** – This port connects the InnGate to the rest of the network for client traffic to pass through.

5. **OPT1** – Used to connect two InnGates in a High Availability (HA) setup. Both OPT1 have to be connected to the same HA VLAN. This will be used for the HA heartbeat signals between the gateways.

6. **Power button** ⏻ (for E Series only) – The power button is located to the left of the front panel, behind the faceplate. The behaviour of the button depends on the power state:

    a. **InnGate is powered up** – Pressing ⏻ will shut down the InnGate.

    b. **InnGate was shutdown normally** – Press ⏻ to power up.

    ⚠ In the event of a power failure, the InnGate will automatically power up when the supply from the electrical mains is restored. The power button does not need to be pressed.

The hardware serial number is usually found on the rear panel of the InnGate and the licensing serial number is accessible via the Admin GUI (see Section 8.11).

1.1.2 Network Operation

As shown in Figure 1-1, the InnGate separates the network into the **upstream** and **downstream** networks:

1. **Downstream Network** – The InnGate manages the Authentication, Authorization and Accounting (AAA) functions and enables the Tru'Connect Zero-Configuration for client devices on the downstream.

2. **Upstream Network** – Only successfully authenticated downstream clients may be authorized to access the upstream network. This is where the server farm, DMZ and also the gateway to the Internet normally reside.

When in operation, the InnGate performs Network Address and Port Translation (NAPT) on the WAN interface for downstream clients (routing can also be done and is discussed in Section 3.2 and Section 3.3). Thus when a downstream client wants to send packets to the upstream, the InnGate will do so using its WAN IP address.

1.2 Recommended Setting

The recommended settings for InnGate 3 are shown in table below:

	M-Series	E-Series	EX-Series
	Recommended	Recommended	Recommended
User Accounts Total number of accounts* + MAC filter entries	1,000	10,000	20,000
Log Entries Total number of log entries in database	5,000	50,000	50,000
User Licenses Total number of detected devices	300	1,000	1,000
VLANs Total number of configured VLANs	300	1,000	2,000
Network Devices Total number of Network devices	30	100	200
Port Binding Rules Total number of Port Binding rules	30	100	200
Undelivered Mails Total number of undelivered mails	1,000	10,000	20,000
Locations Total number of defined Locations	5	15	25
Plans Total number of defined Plans	10	30	50

1.3 System Setup

This section explains the basic configuration for a new InnGate to operate in our network example. These configuration tasks are performed through the web-based admin GUI (see Section 1.3.1):

1. **Configuring the WAN Interface** – See Section 1.3.2.
2. **Configuring the Domain Name Server** – See Section 1.3.3.
3. **Configuring the Web Proxy (optional)** – See Section 1.3.4.
4. **Configuring the Plans** – See Section 1.3.5.
5. **Configuring the Locations** – See Section 1.3.7.
6. **Configuring the VLANs** – See Section 1.3.8.

Some of these tasks can also be performed through the Command Line Interface (CLI) and is discussed separately in the **InnGate Command Line Reference**.

1.3.1 Accessing the Web-based Admin GUI

This section explains how to access[1] the Web-based Admin GUI to configure the system settings.

Power up the InnGate and connect to either the WAN or LAN port using a cross-cable. Then follow the instructions to access the Admin GUI:

> ⚠ If ever you are unable to access the InnGate from one of the interfaces due to possible incorrect configuration settings, you can always attempt to reconnect via the other interface. In addition, the Admin GUI can only be accessed via secure-HTTP (HTTPS) and the forward slash ('/') after "admin" should be included.

1. **Connecting from the WAN Interface:**

   The URL to access the Admin GUI is:

   `https://<WAN IP Address>/admin/`

   ⚠ The factory default WAN IP address is **192.168.0.1**, with a subnet mask of **255.255.255.0**. When connecting directly, ensure that the subnet mask setting on your client device matches the default value. The URL of the Admin GUI for a new InnGate will therefore be: **`https://192.168.0.1/admin/`**

2. **Connecting from the LAN Interface:**

   The URL to access the Admin GUI is:

   `https://ezxcess.antlabs.com/admin/`

   ⚠ The "ezxcess.antlabs.com" domain is only valid on the LAN network (assuming that LAN access to the Admin GUI is not blocked) and is not a valid domain on the public Internet.

Figure 1-4 shows the SSL warning message you will see when connecting via HTTPS. Click the **Yes** button to continue.

[1] You will need a version 4.0 or better MS IE/Netscape web browser to access the Admin GUI. The web browser should also have cookies and Javascript enabled and must support frames.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 1-4 SSL Warning Message

The administrator's login page is presented next (see Figure 1-5).

Figure 1-5 Login Prompt

*Login with the default User ID "**root**" and default password "**admin**".*

⚠ It is recommended that you change the default password (see Section 8.3.2) to prevent unauthorized access.

Upon successful login, the main Admin Page will be displayed (Figure 1-6 shows a portion of the actual page), which is a status summary.

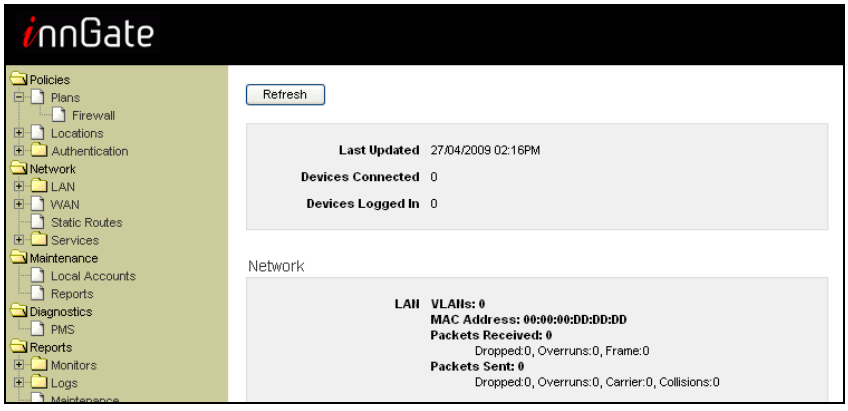
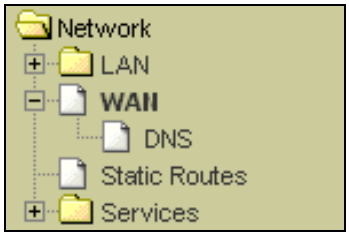


Figure 1-6 Admin Page

The various menu options are displayed on the left side of the page and you may return to the main Admin page at any time by clicking on the "**InnGate**" logo at the top-left corner of the browser window.

1.3.2 Configuring the WAN Interface

The WAN interface has to be properly configured with a routable IP address, valid subnet mask and gateway in order for the InnGate to function correctly in your network.



To configure the WAN Interface:

1. Click on **WAN**.

A list of WAN profiles will be displayed (see Figure 1-7).

Name	IP Address	Subnet Mask	Gateway	Download Limit	Upload Limit	Source NAT Address Range	Description
WAN Interface	10.30.1.89	255.255.255.0	10.30.1.254	Unlimited	Unlimited		WAN Interface

Figure 1-7 WAN Profiles

The InnGate comes preconfigured with a single default WAN profile. In our example, we will go ahead and modify this profile by clicking on the entry.

The settings of the selected WAN Profile will be displayed (see Figure 1-8).

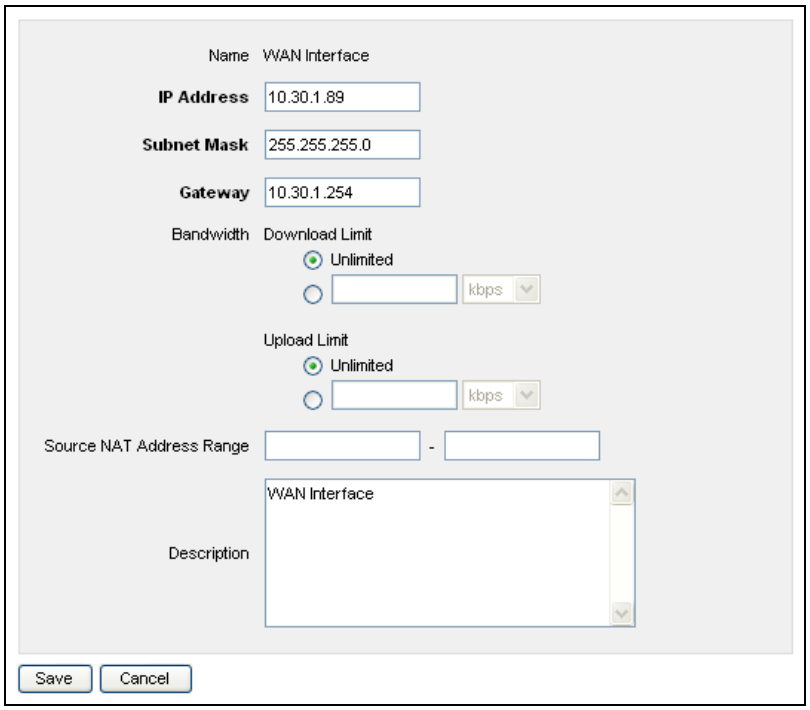


Figure 1-8 Modify WAN Profile

The various fields are described as follows:

1. **IP Address** – The host IP address for the InnGate on the upstream network.

   The factory default IP address setting is `192.168.0.1`. Change this to a valid routable IP address on your upstream network.

2. **Subnet Mask** – The subnet mask of the upstream network that the InnGate is connected to.

   The factory default subnet mask setting is `255.255.255.0`. Change this to the mask used on your upstream network segment.

3. **Gateway** – The address of the router or gateway for the InnGate to send network traffic to for the next-hop.

4. **Bandwidth** – Bandwidth options are available with an optional module which may be purchased separately.

   a. **Download Limit** – The maximum bandwidth allocated for the WAN Interface for incoming packets.

   b. **Upload Limit** – The maximum bandwidth allocated for the WAN Interface for outgoing packets.

5. **Source NAT Address Range** – The InnGate will use the pool of IP addresses defined here when performing network address and port translation (NAPT) on the WAN interface for its downstream clients.

   ⚠ The WAN IP address must be in the same subnet as the source NAT address range

6. **Description** – A description of this profile.

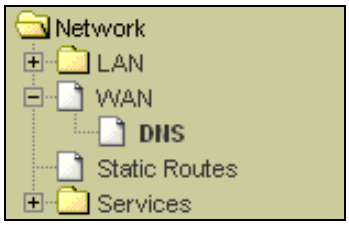
Click Save to confirm the changes. The system will then display a summary of the WAN profile.

⚠ If you are accessing the Admin GUI via the WAN interface and your web browser appears to have stalled, it is because the browser is trying to access the InnGate using the previous IP address. If that happens, close ALL currently opened browser sessions, start a new browser session and login to the admin page again.

1.3.3 Configuring the Domain Name Server

A DNS is required by the InnGate to resolve domain names. If you do not configure this parameter, hosts will only be addressable via their IP addresses.

⚠ If you have your own DNS within your network for name resolutions, you can likewise configure the InnGate to use it. This DNS should be able to resolve both internal and external domains. Alternatively, you can configure the InnGate to use your ISP's DNS for name resolutions. The InnGate also allows more than one DNS entry to be specified.



To configure the DNS settings:

1. Click on **WAN**.
2. Click on **DNS**.

A list of DNS entries will be displayed (see Figure 1-9), sorted in order of priority.

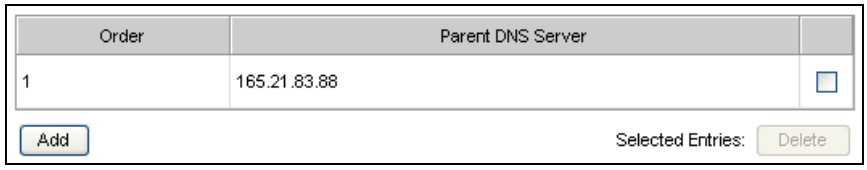


Figure 1-9 DNS Settings

The InnGate comes with a default entry which we will modify according to your network DNS defined. Click on the entry to proceed.

The **DNS** configuration page will be displayed (see Figure 1-10).

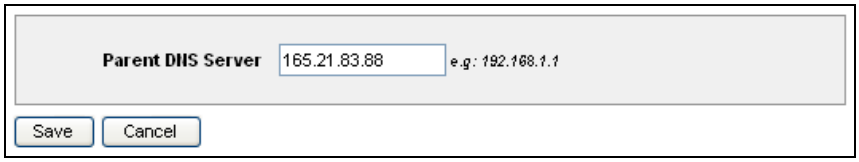


Figure 1-10 DNS Configuration Page

The fields are described here:

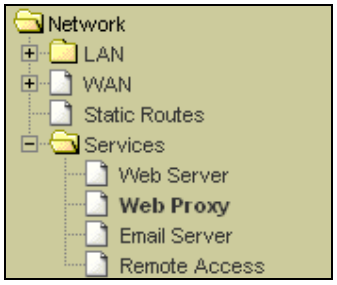
1. **Parent DNS Server** – IP address of the Domain Name Server that can be contacted for name resolution. Click Add to add more entries.

Click Save to confirm the changes.

⚠ The InnGate will switch to another DNS server in the list for subsequent name resolution attempts if a previous attempt was unanswered.

1.3.4 Configuring the Web Proxy

The InnGate can be configured to forward HTTP requests to a web proxy server if necessary. This is **optional**, depending on whether your network allows direct connections to the Internet or requires the use of a proxy.



To configure the Web Proxy settings:

1. Click on **Services**.
2. Click on **Web Proxy**.

The **Web Proxy** configuration page will be displayed (see Figure 1-11).

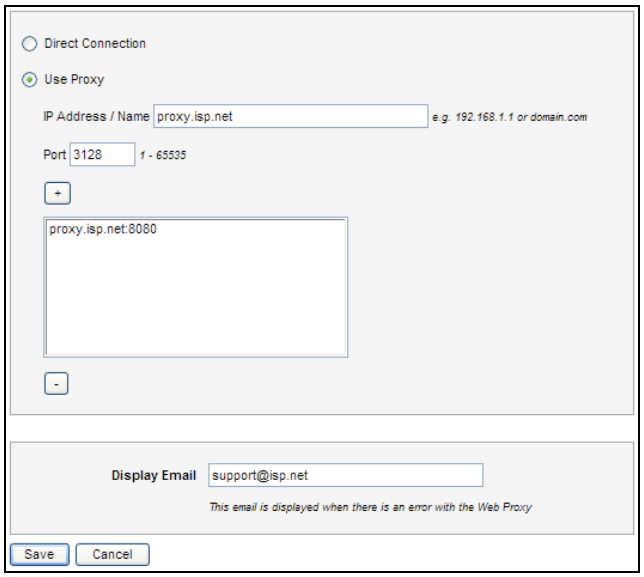


Figure 1-11 Web Proxy Configuration

The various fields are described as follows:

1. **Direct Connection** – Select this if your network allows direct connections to the Internet.

2. **Use Proxy** – Select this if your network requires the use of a web proxy for browsing.

3. **IP Address / Name** – A proxy server entry that the InnGate can use for downstream web traffic.

4. **Port** – The port number for accessing the proxy server.

5. **Display Email** – This is the email address that is displayed in error pages generated when users attempt to access an invalid or inaccessible URL.

You may add and remove proxy server entries by clicking + or -.

Click Save to confirm the entries.

⚠ Configuring the web proxy for the InnGate does not mean that the downstream clients have to set their browser's proxy setting. Downstream clients will continue to enjoy Zero-Configuration. However, it is important to note that a downstream client that has an existing browser proxy setting (e.g. company laptop with corporate web proxy setting) should not change it after logging in.

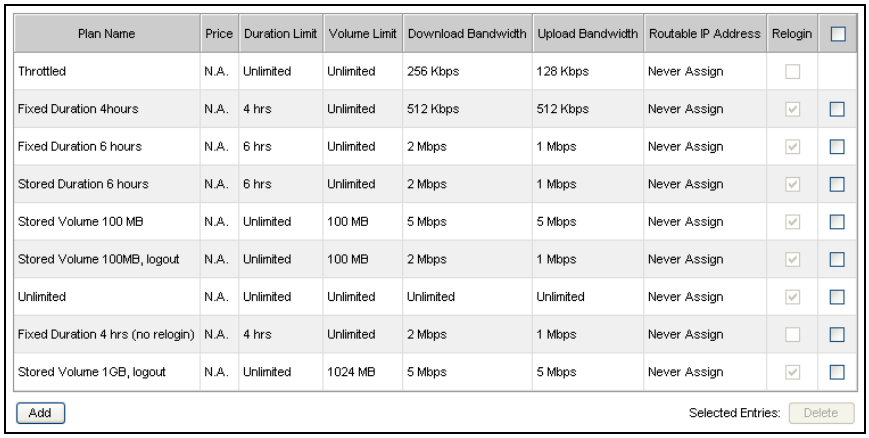
1.3.5 Creating a Plan

Next you need to create the different types of service plans required. This depends on your business needs.

To configure the Plans:

1. Click on **Policies**.
2. Click on **Plans**.

Any existing plans will be shown. Select an existing plan or create a new one.



Plan Name	Price	Duration Limit	Volume Limit	Download Bandwidth	Upload Bandwidth	Routable IP Address	Relogin	
Throttled	N.A.	Unlimited	Unlimited	256 Kbps	128 Kbps	Never Assign	☐	
Fixed Duration 4hours	N.A.	4 hrs	Unlimited	512 Kbps	512 Kbps	Never Assign	☑	☐
Fixed Duration 6 hours	N.A.	6 hrs	Unlimited	2 Mbps	1 Mbps	Never Assign	☑	☐
Stored Duration 6 hours	N.A.	6 hrs	Unlimited	2 Mbps	1 Mbps	Never Assign	☑	☐
Stored Volume 100 MB	N.A.	Unlimited	100 MB	5 Mbps	5 Mbps	Never Assign	☑	☐
Stored Volume 100MB, logout	N.A.	Unlimited	100 MB	2 Mbps	1 Mbps	Never Assign	☑	☐
Unlimited	N.A.	Unlimited	Unlimited	Unlimited	Unlimited	Never Assign	☑	☐
Fixed Duration 4 hrs (no relogin)	N.A.	4 hrs	Unlimited	2 Mbps	1 Mbps	Never Assign	☐	☐
Stored Volume 1GB, logout	N.A.	Unlimited	1024 MB	5 Mbps	5 Mbps	Never Assign	☑	☐

Add — Selected Entries: Delete

Figure 1-12 Plans

Figure 1-13 shows the plan creation page. These are the fields:

1. **Plan Name** – Name of the plan. Best to give a meaningful name.
2. **Price** – The units to charge for usage. The definition of a unit depends on what is defined in your PMS system.
3. **Duration & Volume Limit** – Select if you want to charge by duration or data volume usage. The user will need to repurchase once the plan is used up. The 4 different types of duration and volume plans supported are:

    a. **Unlimited duration and volume**

    b. **Fixed Duration / Single Duration** – single fixed usage period valid from the first time of use for the duration specified

    c. **Stored Duration** – multiple usage period valid as long as there is balanced time left

⚠ You need to purchase the Stored Volume Prepaid module in order for this option to be enabled.

d. **Stored Volume** – multiple usage periods valid as long as there is balanced volume left.

i. **Change users to Throttled plan after volume is exceeded** –

If this option is unchecked, then the user is immediately logged out from the system when the volume limit is exceeded.

If this option is checked, then the user's bandwidth will be changed to that specified in the 'Throttled' plan once the volume limit is exceeded. The user can continue to use the system until he logouts or departs from the network, after which the account cannot be used for login anymore.

⚠ There is a default **Throttled** Plan that is pre-configured in the Gateway. The user's bandwidth will be automatically adjusted to the values specified in this plan if the user's plan is a volume plan with the throttled option enabled and the volume limit is exceeded. The default bandwidth for this plan is unlimited. You will need to change it to your desired throttled value if you want to use this feature.

4. **Upload / Download Bandwidth** – Set the bandwidth limits here.

5. **Routable IP Address** – Select if you want to allow users to request for a public IP address. Useful if the user has some applications that need it or cannot work in a NAT environment.

6. **Attempt to reconnect users**... – Select this if you want to enable cookie-based relogin so that users need not keep going through the welcome login page for separate sessions of usage.

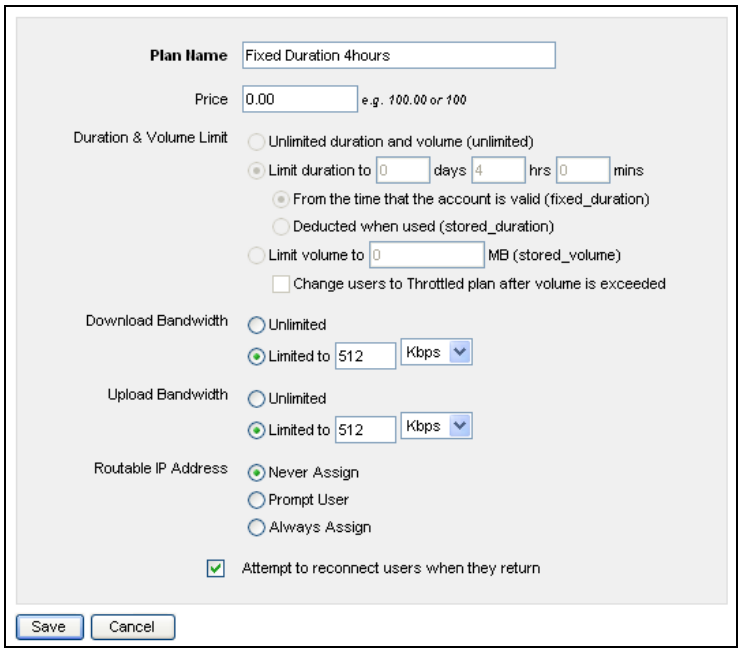


Figure 1-13 Creating a Plan

Click Save to confirm the changes.

1.3.6 Firewall Rules

The InnGate allows you to define firewall-like rules that can be applied to individual User Groups for greater control over network access.

To configure a Firewall rule:

1. Click on **Plans.**
2. Click on **Firewall**.

Any existing entries will be displayed (see Figure 1-14). Any account belonging to the Plan will be subject to the rules defined in the order that the rules appear when they log in.

Click on an entry to modify it or click Add to create one.

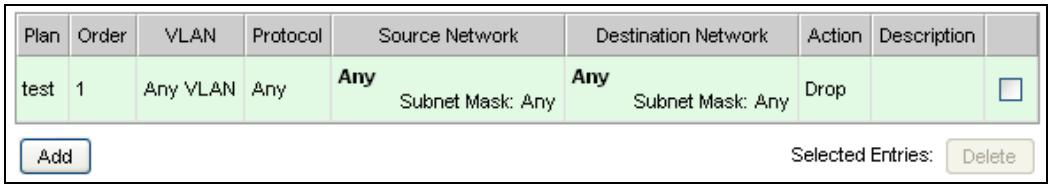


Figure 1-14 List of Firewall rules

The **Firewall** rule definition page will be displayed (see Figure 1-15).

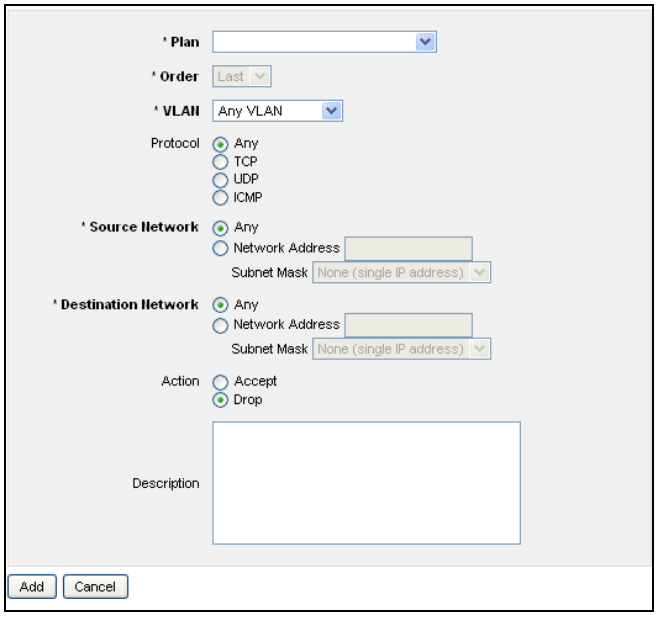


Figure 1-15 Plan Firewall

The fields are described as follows:

1. **Plan** – The Plan that this firewall rule will apply to.

⚠ You can also configure Firewall rules for the following default groups of devices:

- **Blacklisted Devices** – users whose MAC addresses are denied access. Section 2.6.
- **Whitelisted Devices**– users whose MAC addresses are allowed access without login. Section 2.6.
- **Throttled** – users who are throttled.
- **None** – users who are not login yet.

2. **Order** – The position in the list of rules and determines its priority.

3. **VLAN** – The firewall rule will be applied to users that connect from the specified VLAN group. Previously defined VLAN Groups will appear here along with the following additional options:

    a. **Any VLAN** – Applies to traffic from any VLAN.

b. **No VLAN** – Applies to traffic that has no VLAN tag.

4. **Protocol** – This specifies the type of network traffic that the firewall will pick up.

5. **Source Network** – The firewall will pick up network traffic originating from the specified IP address or network.

6. **Source Port** – The firewall will pick up network traffic with the specified source port number.

7. **Destination Network** – The firewall will pick up network traffic heading for the specified IP address or network.

8. **Destination Port** – The firewall will pick up network traffic with the specified destination port number.

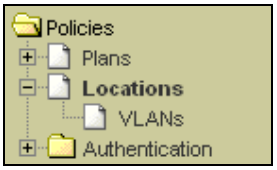
9. **Action** – This is the action that will be performed for network traffic that is picked up by the firewall based on the above specified criteria.

10. **Description** – A description for the firewall rule.

Click Add to confirm the entry (or Save for modifications).

1.3.7 Creating a Location

Now partition your network into service locations and attach the different plans to each location.



To configure the Location:

1. Click on **Locations**.

A list of locations will be displayed (see Figure 1-16). Any other locations added later will also be listed here.

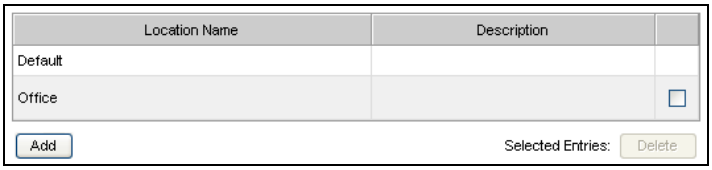


Figure 1-16 Creating a Location

The InnGate comes preconfigured with a default location.

After making a selection, details about the location is displayed (see Figure 1-17).

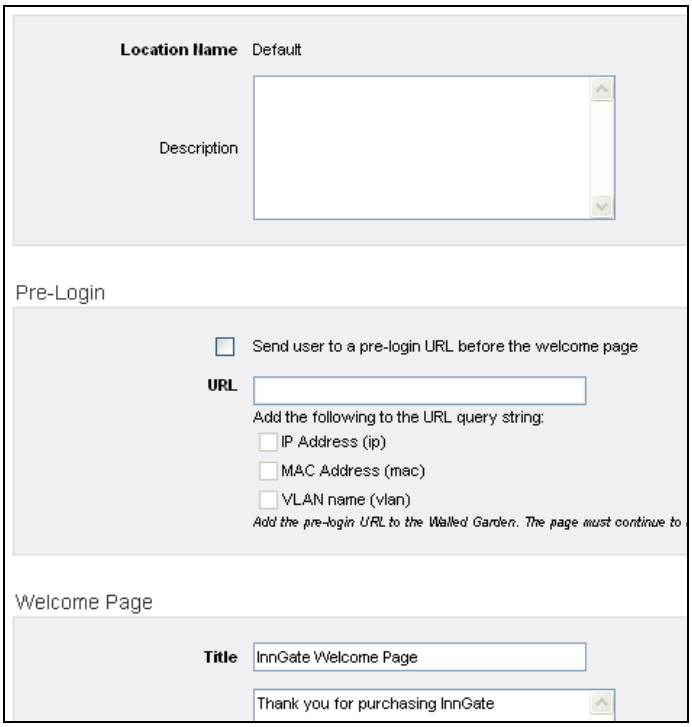


Figure 1-17 Location Settings

Creating a location is a multi-step process and the wizard will guide you through the steps.

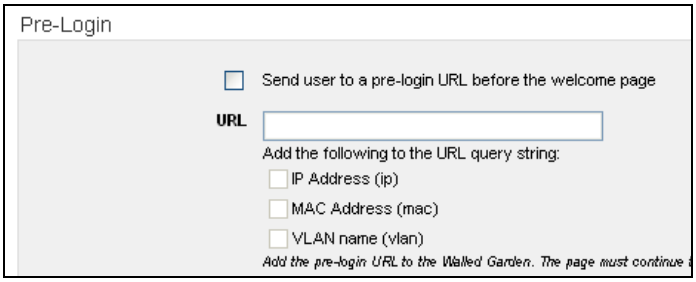

Pre-Login
Send user to a pre-login URL before the welcome page
URL
Add the following to the URL query string:
IP Address (ip)
MAC Address (mac)
VLAN name (vlan)
Add the pre-login URL to the Walled Garden. The page must continue

Figure 1-18 Pre-Login Page

The Pre-Login section lets you configure what page is shown to the user instead of the login page. Enable the check box to turn on this feature.

1. **URL** – This is the URL of the page to send the user to. In addition, you can pass the zero-configuration settings to this webpage and do customized processing.

⚠ When using a pre-login page, make sure it eventually sends the user to the welcome page to login.

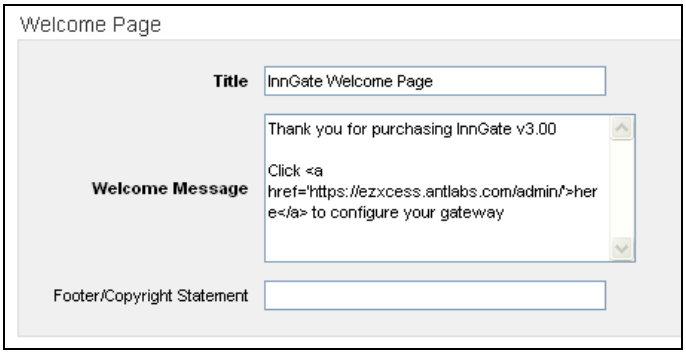


Figure 1-19 Welcome Page

The Welcome Page section lets you configure how the welcome login page will look like.

1. **Title** – The title of the page shown in the browser.

2. **Welcome Message** – The content shown on the page. Accepts HTML code.

3. Footer/Copyright Statement – The footer or copyright statement shown at the bottom part of the login page.

The Look & Feel section is meant for customizing the presentation of the landing page, allowing you to modify it via CSS and even uploading your own CSS definitions. This advanced feature is normally used for customized solutions.

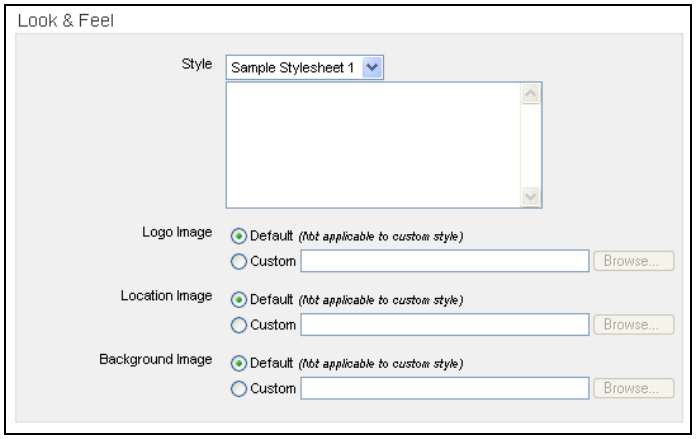


Figure 1-20 Look & Feel Page

Click Next Step » to proceed with the next step in the wizard.

The next step in the wizard allows you to select the different access options available to users in this location you are creating:

1. **Complimentary Access** – This means the user will not be charged and there is no need to enter a User ID and Password. Select from the list of plans created previously. The name given for the **Display Label** will be what is shown in the plan selection drop-down box.

   Only Fixed Duration plans with relogin option enabled can be selected as a Complimentary Access plan.

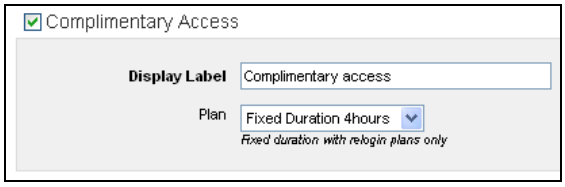


Figure 1-21 Complimentary Access

2. **Local Authentication** – This is the standard User ID and Password login access method.

Figure 1-22 Local Authentication

3. **Radius Authentication** – This is currently not available.

4. **PMS Authentication** – This integrates with the PMS system so that charges will be sent to the PMS and will show up on the final bill as services charged to his room.

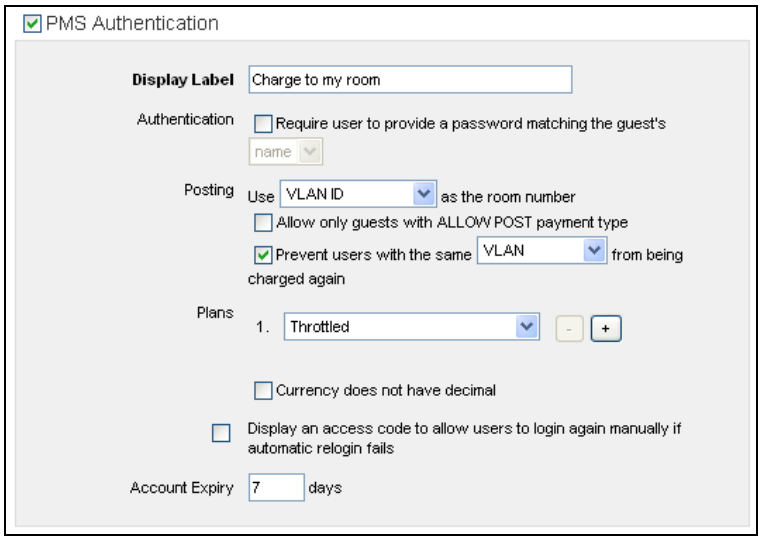


Figure 1-23 PMS Authentication

a. **Display Label**

b. **Authentication –** When this option is checked the guest based authentication is enabled. Guest is required to specify the room number, guest name, or reservation number. If it is unchecked the room based authentication is enabled.

c. **Posting –** VLAN ID, VLAN Name, and Description can be used as the room number for posting.
   - **Allow only guests with ALLOW POST ... -** If it is checked only guests with "Allow Post" status can do posting.
   - **Prevent users with the same ... -** Is checked to prevent double billing.

d. **Plans –** To configure what are the plans selectable in the login page.

e. **Currency does not have decimal –** The billing amount is sent in cent. If it is checked the billing amount will not be multiplied by 100.

f. **Display an access code to ... -** This option is to display an access code so the user can use this access code to do manual login if automatic relogin fails.

g. **Account Expiry –** To specify the validity of the accounts created. The value must be between 1 to 90 days. All expired accounts will be deleted by system maintenance.

5. **Access Code Authentication** – Instead of a User ID and Password system, this only requires an access code to be entered for access.

Figure 1-24 Access Code Authentication

6. **Authentication Display** – Define the order in the drop-down list of authentication options that is shown to the user.

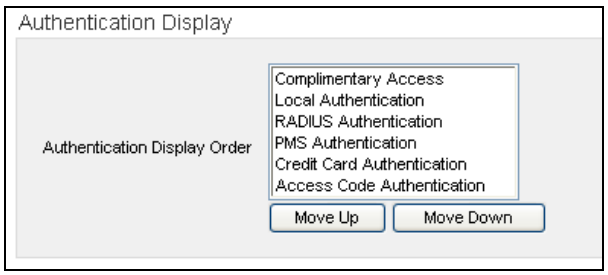


Figure 1-25 Authentication Display

Click Next Step » to proceed with the next step in the wizard.

The next step in the wizard will let you define the content that is shown under the terms and conditions.

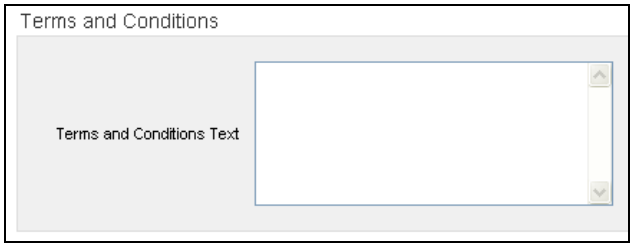


Figure 1-26 Authentication Display

Click Next Step » to proceed with the next step in the wizard.

The next step is to define what is shown to the user when he successfully authenticates.

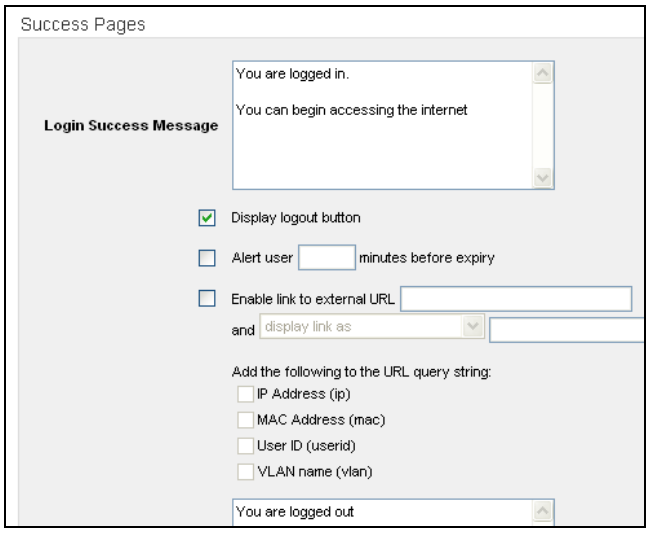


Figure 1-27 Success Pages

These are the fields:

1. **Login / Logout Success Message** – The messages shown to the user.

2. **Display Logout Button** – To show the button for logging out of the session. Useful for time duration based plans.

3. **Alert user**... – A timer will show on the page indicating the amount of time left. Useful for time duration based plans.

4. **Enable link** to external URL – To include customized post-login processes, enable this to invoke the following actions to an external page.

    a. **display link as** – the external page is displayed as a link on the default success page

    b. **redirect to link after** – the default success page is first shown for the specified number of seconds before redirecting to the external page

    c. **use link as login success page** – the external page is used as the success page.

    d. **Add the following to the URL query string** – You can also choose to pass the zero-configuration variables, such as IP address, MAC address, User ID to the external page for advanced integration requirements.

Click Next Step > to proceed with the next step in the wizard.

The next step is to define what is shown to the user if the system encounters an error.

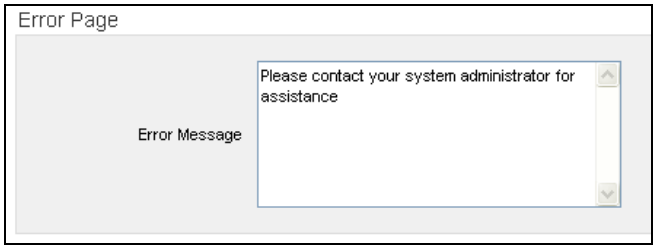


Figure 1-28 Error Page

Click Next Step > to proceed with the next step in the wizard.

The next step is to define what to name the various labels on the pages shown to the user in the whole authentication process.

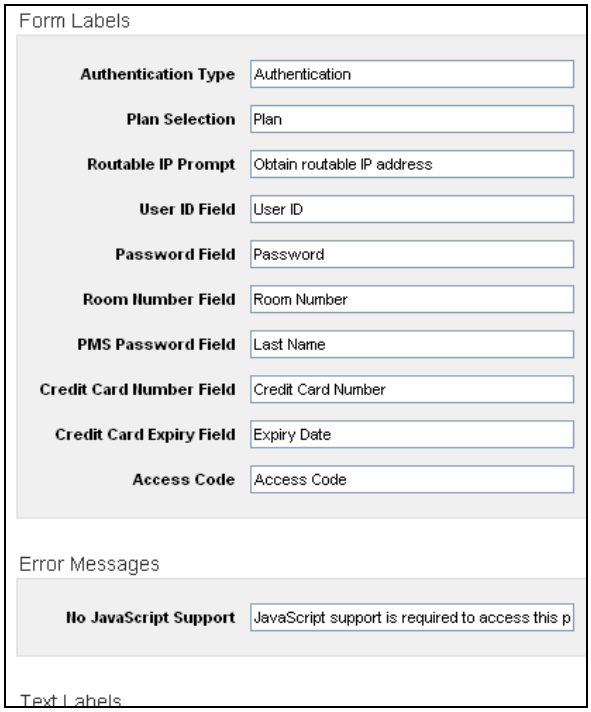


Figure 1-29 Customizing Labels

Click Next Step > to proceed with the next step in the wizard.

The next step allows you to preview the Welcome Login page that you have just configured.

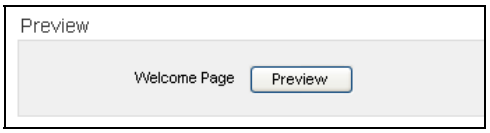


Figure 1-30 Error Page

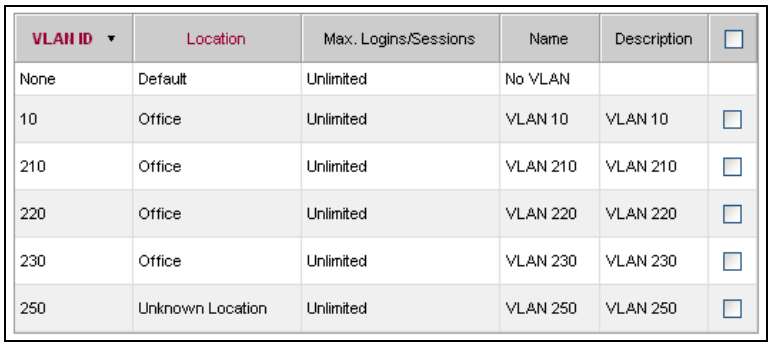
At any step in the wizard, you can always click Save to confirm the changes.

1.3.8 Creating VLANs

Within each location, you will now assign VLANs to it so that under each VLAN you can have network specific controls.

To configure the VLAN:

1. Click on **Locations**.
2. Click on **VLANs**.



VLAN ID	Location	Max. Logins/Sessions	Name	Description	
None	Default	Unlimited	No VLAN		
10	Office	Unlimited	VLAN 10	VLAN 10	☐
210	Office	Unlimited	VLAN 210	VLAN 210	☐
220	Office	Unlimited	VLAN 220	VLAN 220	☐
230	Office	Unlimited	VLAN 230	VLAN 230	☐
250	Unknown Location	Unlimited	VLAN 250	VLAN 250	☐

Figure 1-31 VLANs

Figure 1-31 shows the list of existing VLANs. Select an existing record or create a new one.

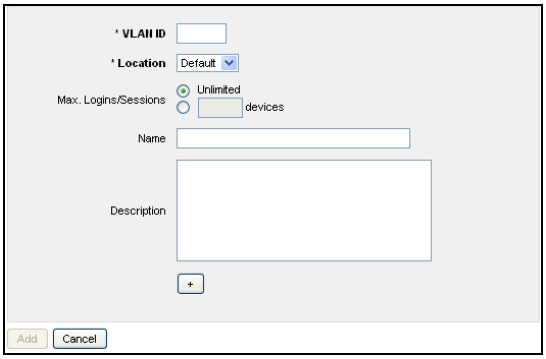


Figure 1-32 Defining a VLAN

The fields are described as follows:

1. **VLAN ID** – Unique VLAN identifier. Must correspond to the VLAN setup in the switch connected via the trunk port.

2. **Location** – Select the Location that this VLAN belongs to.

3. **Max. Logins/Sessions** – The maximum number of concurrent users allowed on the VLAN.

4. **Name** – The name given to this VLAN definition.

5. **Description** – A description for this VLAN.

Click + (below the **Description** field) to create the VLAN entry and it will be displayed in a table (see Figure 1-33).

Figure 1-33 New VLAN entry created

You can add more entries or click on the respective - buttons to remove existing entries.

⚠ These VLAN entries are not committed yet. Once you have finalized the list of entries you can proceed to save the list by clicking on the second Add button as shown in Figure 1-34.

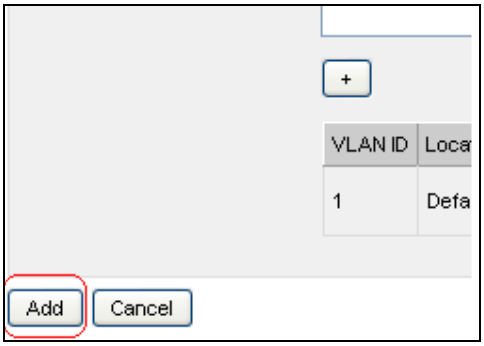


Figure 1-34 Commit the VLAN entries

⚠ You can also import and export VLAN definitions from a file in comma-separated-values format (see Section 1.3.9).

⚠ A default entry treats traffic that is not VLAN tagged ("**No VLAN**") to be assigned to the "**Default**" VLAN Group. You can change this treatment if required.

1.3.9 Importing and Exporting VLAN Definitions

To import/export VLAN definitions:

1. Click on **Locations**.
2. Click on **VLANs**.

Figure 1-35 shows the list of VLAN definitions.

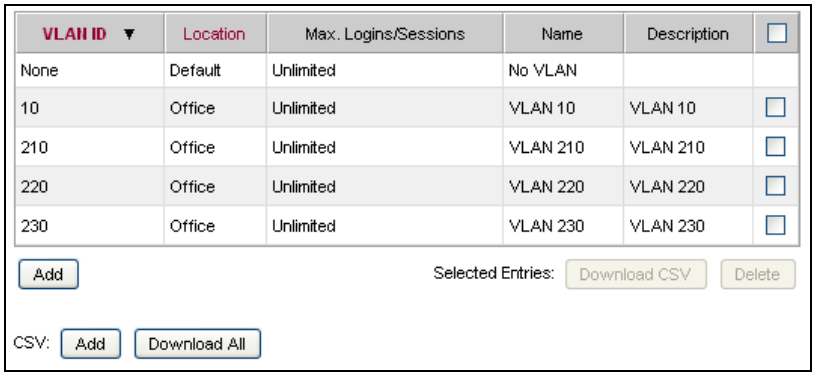


Figure 1-35 Import/Export VLAN Definitions

Click "CSV: Add" to import VLAN definitions from a comma-separated-values formatted file. To export VLAN definitions from the system, check the required entries and click Download All.

⚠ The format of the exported records file may not compatible with older versions of the InnGate.

Figure 1-36 shows the interface for selecting a CSV file to upload.

Figure 1-36 Upload VLAN definitions

Click Browse... to select the file to upload and click Add CSV to begin importing the VLAN definitions.

Errors will be highlighted by the system.

The CSV file must provide these fields enclosed with double quotes, in the following order, separated by commas, and each entry on a separate line:

1. **VLAN ID**
2. **Location**
3. **Max. Logins/Sessions**
4. **Name**
5. **Description**

The following is an example of a single record from a CSV file:

```
"VLAN ID","Location","Max. Logins/Sessions","Name","Description"
"1","e-Services","","Hotspot VLAN",""
```

⚠ The CSV must contain a header row which will not be imported.

1.4 Network Installation

The following steps describe how to install the InnGate in the desired network:

1. **Connect the respective network cables to the InnGate:**
    a. **LAN interface** – Connect to the downstream network.
    b. **WAN interface** – Connect to the upstream network.
2. **Power up the InnGate**.
    a. Connect the InnGate to the electrical mains using the power cable.
    b. Turn on the power supply from the mains.
    c. Press the power button ⏻ to start up the InnGate.

Warning: Connecting the wrong interface to the network can result in downtime to your existing network.

1.4.1 VLAN-enabled Networks

When incorporating the InnGate in a VLAN-enabled network, the LAN interface must connect to an 802.1Q-enabled trunk port on the switch.

This trunk port should receive all tagged VLAN traffic from downstream clients that are to be managed by the InnGate. The InnGate will then be able to apply location specific policy settings based on the VLAN information for each client.

In addition, the InnGate must be configured to recognize the VLAN setup and this is covered in Section 1.3.8.

1.5 Testing the Configuration

The InnGate is now configured and ready to accept client connections on the LAN interface. Follow the steps below to connect a client on the downstream to the Internet via the InnGate.

1. Connect a PC/Laptop on the downstream. One way to do this is to connect directly to the LAN interface (you must use a cross-cable for a direct client to InnGate connection) which may be useful for quick demonstrations.

2. Startup the Internet browser on the connected computer.

3. Attempt to access the URL of a valid website with the browser. Up to this point, you have basically simulated a typical user connecting to your downstream LAN to connect to the Internet through the InnGate.

4. If the configuration is done correctly, you will be able to access the website and see the configured login page as shown in Figure 1-37.

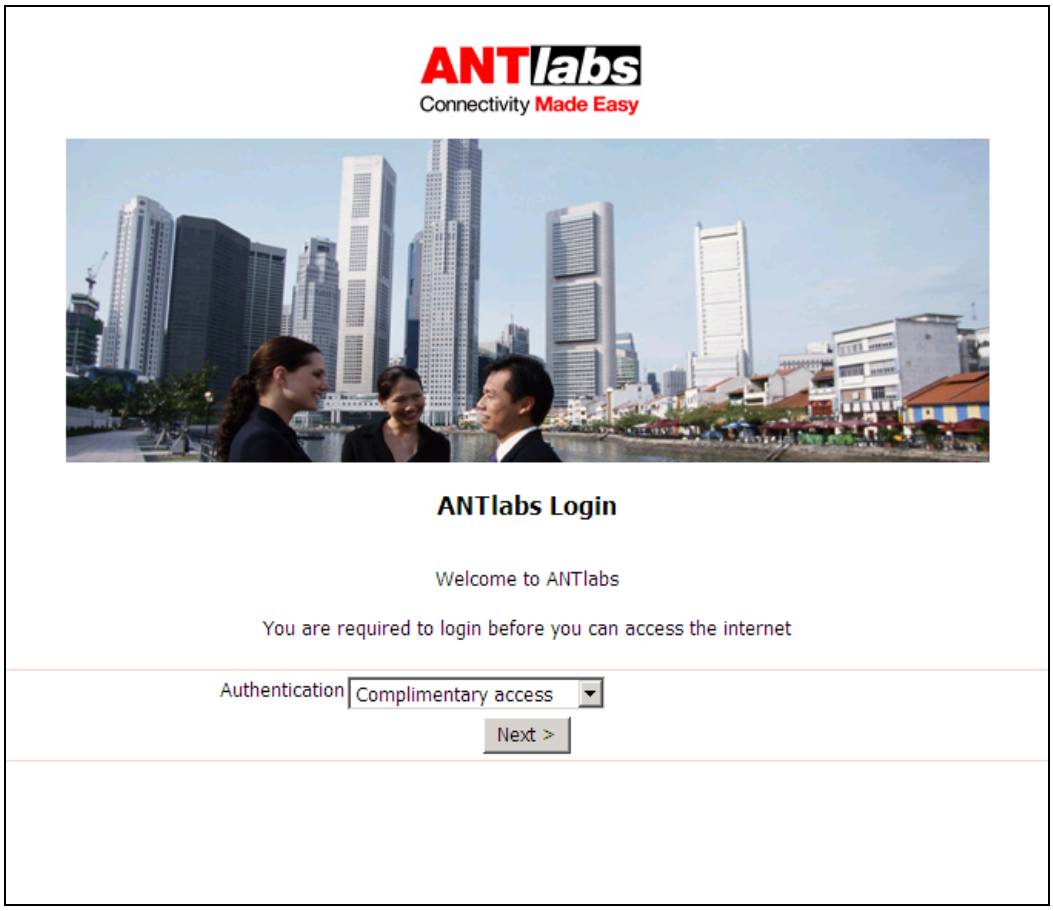


Figure 1-37 Login Page

⚠ If you are unable to surf to the website, check that the instructions in the previous sections were implemented correctly.

Chapter 2

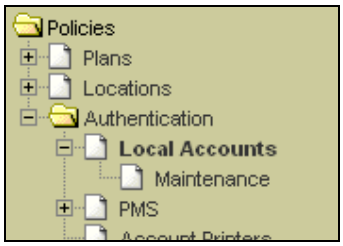
Authentication

2.1 Overview

This chapter explains how to configure the different authentication methods that you can use for the range of services you want to provide.

2.2 Local Accounts

Use this to create local User ID and Password accounts to be given out to users. Users will then use it to login.



To access the option:

1. Click on **Authentication**.
2. Click on **Local Accounts**.

Any existing accounts will be shown as seen in Figure 2-1. Click an existing record to edit or add a new one.

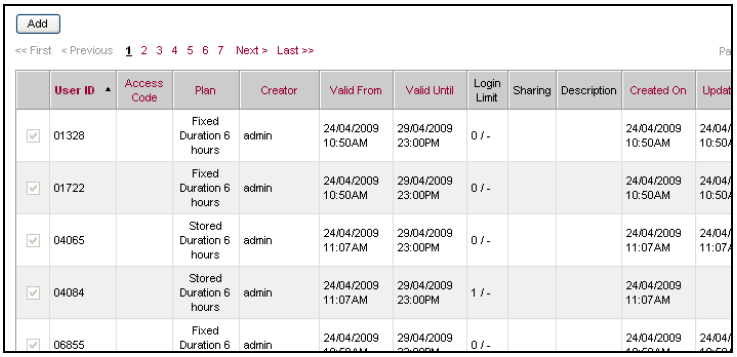

Add
<< First < Previous 1 2 3 4 5 6 7 Next > Last >>
User ID
Access Code
Plan
Creator
Valid From
Valid Until
Login Limit
Sharing
Description
Created On
01328 Fixed Duration 6 hours admin 24/04/2009 10:50AM 29/04/2009 23:00PM 0 / - 24/04/2009 10:50AM
01722 Fixed Duration 6 hours admin 24/04/2009 10:50AM 29/04/2009 23:00PM 0 / - 24/04/2009 10:50AM
04065 Stored Duration 6 hours admin 24/04/2009 11:07AM 29/04/2009 23:00PM 0 / - 24/04/2009 11:07AM
04084 Stored Duration 6 hours admin 24/04/2009 11:07AM 29/04/2009 23:00PM 1 / - 24/04/2009 11:07AM
06855 Fixed Duration 6 admin 24/04/2009 29/04/2009 0 / - 24/04/2009

Figure 2-1 Existing accounts

When creating a new record, select either to create a single account or multiple accounts at once.

Figure 2-2 Account Creation

The sections are described as follows:

1. **Type** – Select whether you want to create a User ID and Password based login account or an Access Code account which only requires the user to enter the code to login.

2. **Sharing** – Select whether more than one device can login and use the service at the same time with the same account.

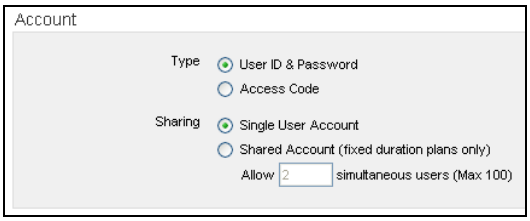


Figure 2-3 Account Type

3. **Credentials** – The User ID and Password.

Figure 2-4 Account Credentials

4. **Plan** – Select the type of Plan that the account is being created for. The Plans should already have been created at the start when configuring the service offerings.

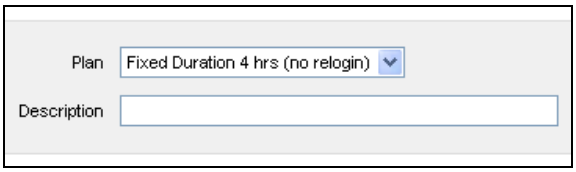


Figure 2-5 Plan Type

5. **Advanced Subsection** – Under the advanced subsection, there are additional account control options:

    a. **Account can be used…** – You can set the time when the account will start being usable. Useful for accounts created ahead of time for a future event.

    b. **Expire the account after…** – You can also set the validity period here.

c. **Limit logins to...** – Here you can further restrict how many logins are allowed before the account is no longer valid.

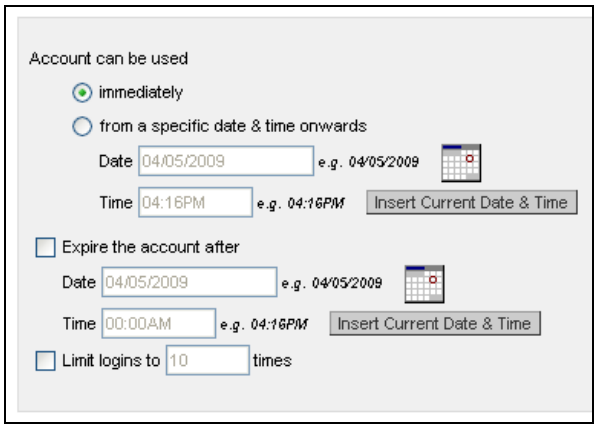

Account can be used
immediately
from a specific date & time onwards
Date 04/05/2009 e.g. 04/05/2009
Time 04:16PM e.g. 04:16PM Insert Current Date & Time
Expire the account after
Date 04/05/2009 e.g. 04/05/2009
Time 00:00AM e.g. 04:16PM Insert Current Date & Time
Limit logins to 10 times

Figure 2-6 Advanced Subsection

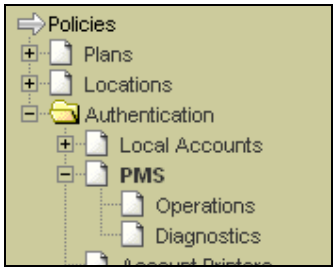
Click Save to commit the changes.

2.2.1 Local Accounts Maintenance

Local Accounts Maintenance is explained in details in Section 6.2.

2.3 PMS

Use this to interface with a PMS system.



To access the option:

1. Click on **Authentication**.
2. Click on **PMS**.

The InnGate comes with various pre-built interfaces for common PMS. Select the correct one.

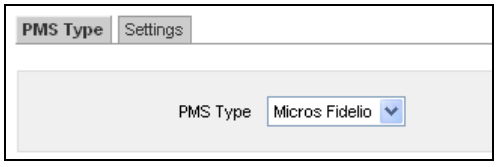


Figure 2-7 PMS Type

⚠ When you change the PMS type you need to re-save Location's PMS Authentication setting to associate new PMS configuration.

Next, configure the interface parameters according to the setup of the PMS so that the InnGate can communicate with the PMS for authentication and accounting of usage.

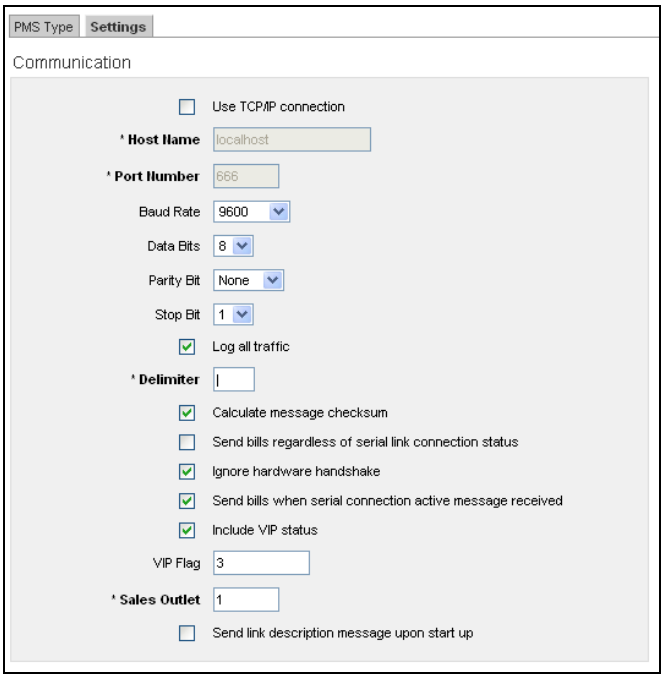


Figure 2-8 PMS Communication Setting

1. **Use TCP/IP connection –** To enable TCP/IP based PMS.
2. **Host Name –** The host name used for TCP/IP connection.
3. **Port Number –** The port number used for TCP/IP connection.
4. **Baud Rate –** Serial baud rate.
5. **Data Bits –** It is necessary to set 8 as number of data bits to be able to transmit multiple character sets.
6. **Parity Bit –** To enable single bit error correction. The default is None.
7. **Stop Bit –** The default value is 1.
8. **Log all traffic –** This option is to enable or disable detailed PMS traffic logging.

9. **Delimiter –** To specify the field separator in the PMS data stream. The default is bar character "|".

10. **Calculate message checksum –** To include LRC checksum of the message at the end of the data stream.

11. **Ignore hardware handshake –** To turn on or off the hardware handshake.

12. **Sales Outlet –** This is sent during posting to identify different type of services or posting. This is only used by TCP/IP based Micros Fidelio.

Figure 2-9 shows the PMS Billing Setting.

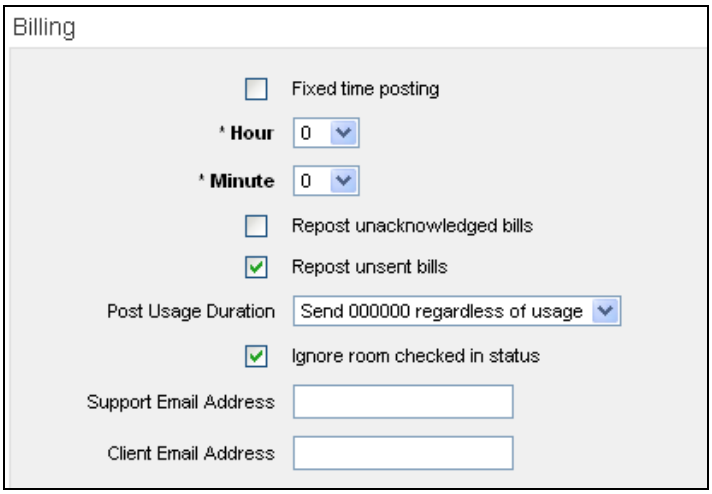


Figure 2-9 PMS Billing Setting

1. **Fixed time posting -** To enable or disable fixed time bill posting.

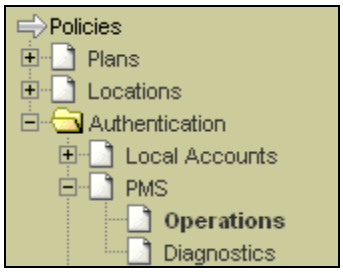
2. **Repost unacknowledged bills –** To enable or disable reposting of unacknowledged bills.

3. **Repost unsent bills –** To enable or disable resposting of unsent bills.

4. **Post Usage Duration –** To configure the duration value when overflow usage happens.

Click Save to commit the changes.

Once configured, you can also trigger operational events and perform diagnostics via the PMS interface.



To access the option:

1. Click on **Authentication**.
2. Click on **PMS**.
3. Click on **Operations**.

This allows you to generate a check in or check out event.

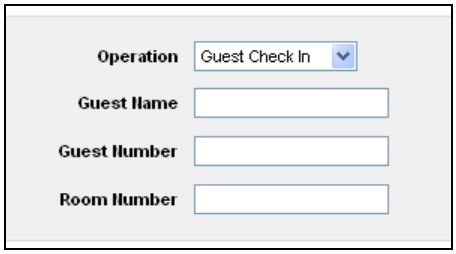
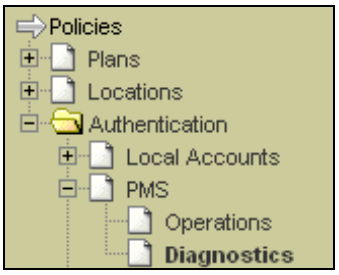


Figure 2-10 PMS Operation

You can also use the diagnostic tool to post PMS events.



To access the option:

1. Click on **Authentication**.
2. Click on **PMS**.
3. Click on **Diagnostics**.

Enter the PMS post event details and you can use it to test if the PMS posting from the InnGate works correctly. The details can be found in Section 6.4.

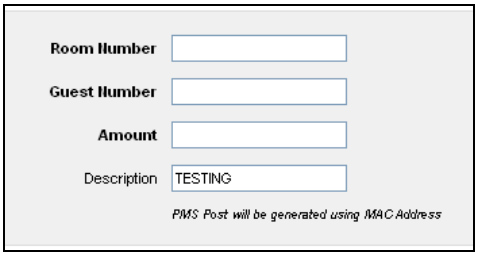
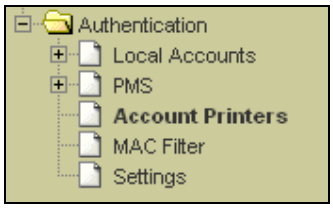


Figure 2-11 PMS Diagnostics

2.4 Account Printers

Use this to configure account printer-based authentication.



To access the option:

1. Click on **Authentication**.
2. Click on **Account Printers.**

Enter the printer's IP address and click button Add.

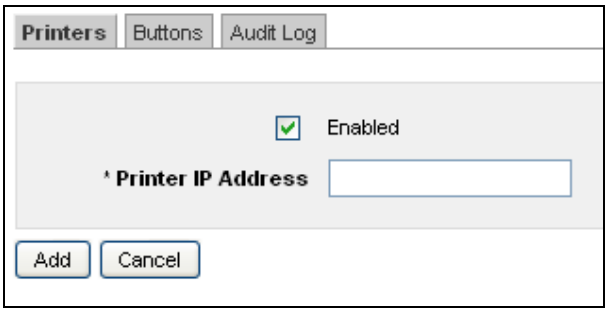


Figure 2-12 Account Printers Authentication

Next step is to configure each button of the account printer. There is a maximum of six buttons supported. Click on the button you want to configure.

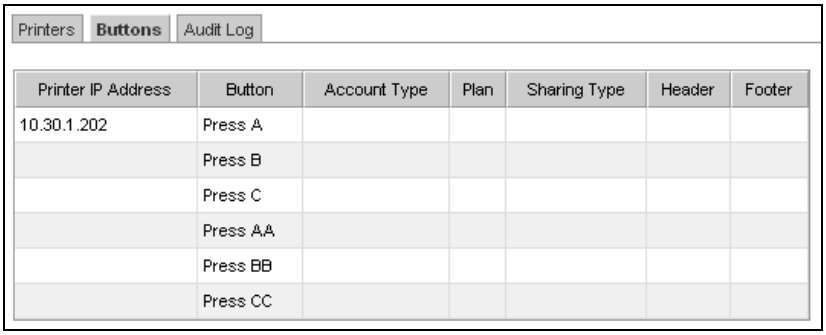


Figure 2-13 Account Printers Button Setting

Choose the account type and account sharing option you want to assign to the respective button. Shared account is only applicable to fixed duration plans and it only allows maximum 100 simultaneous users.

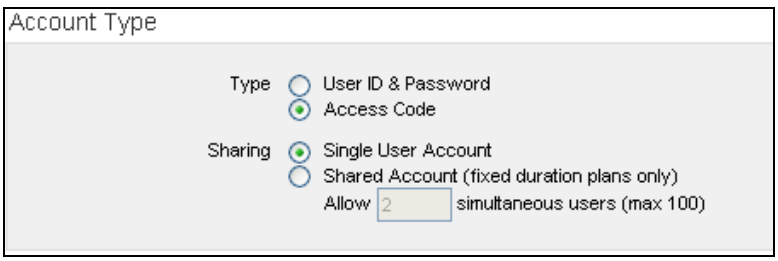


Figure 2-2-14 Account Type

If the account type is User ID & Password the Credentials setting will be shown in Figure 2-15.

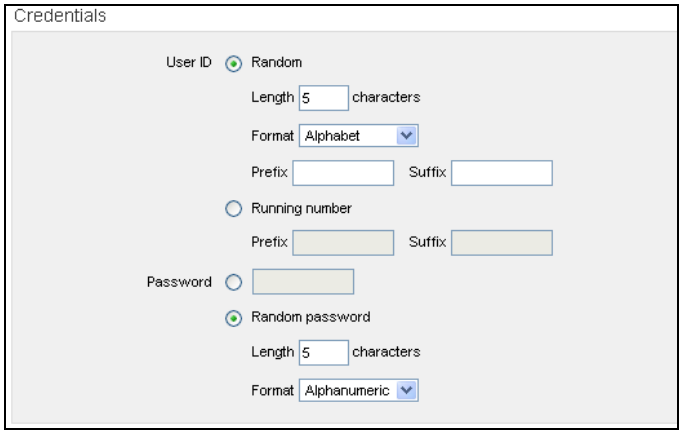


Figure 2-15 User ID & Password's Credentials

If the account type is Access Code the Credentials setting will be shown in Figure 2-16.

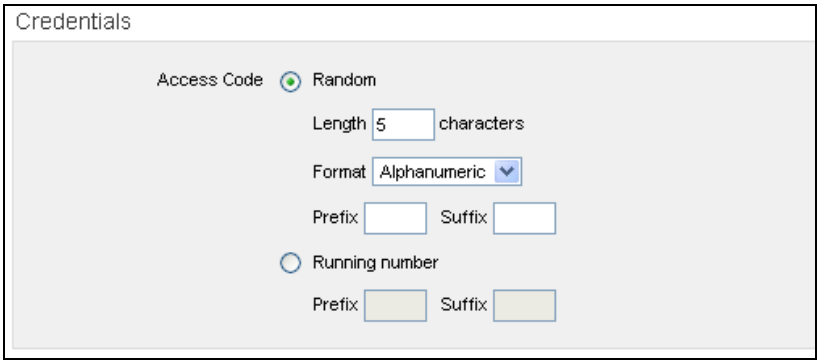


Figure 2-16 Access Code's Credentials

Configure the plan, account expiry and the login limit to be assigned to the accounts created by respective button.

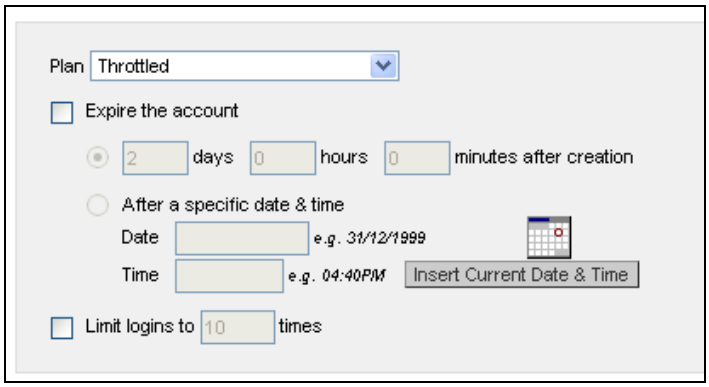


Figure 2-17 Account configuration

Enter the header and footer text to be printed by account printer.

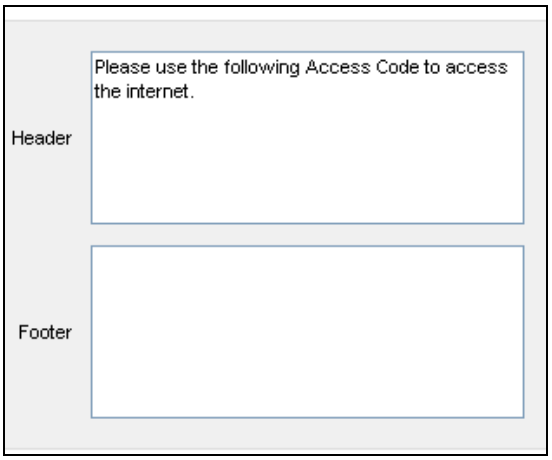


Figure 2-18 Header and Footer

Click button Save to save the configuration.

Use Audit Log to view the accounts created.

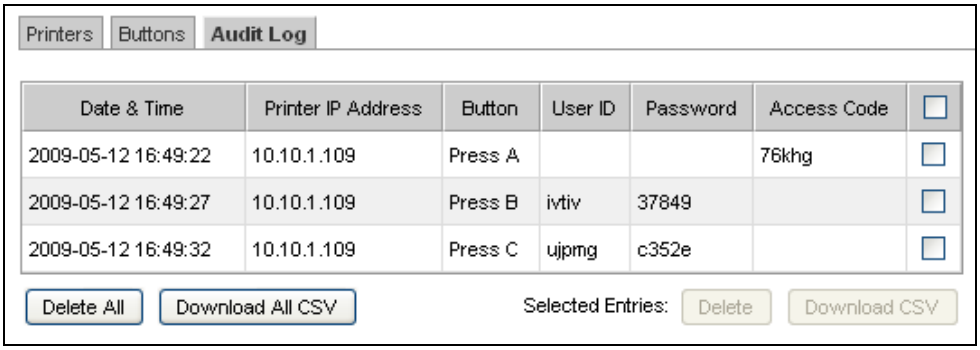
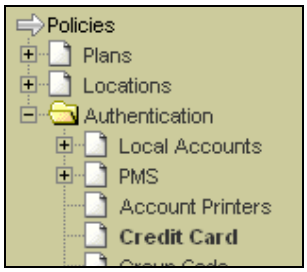


Figure 2-19 Audit Log

2.5 Credit Card

Use this to allow users to pay for service via credit card.



To access the option:

1. Click on **Authentication**.
2. Click on **Credit Card**.

Select the correct payment gateway service provider from the drop down list.

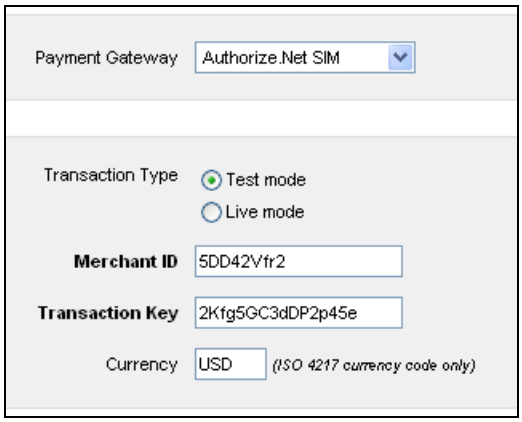


Figure 2-20 Credit Card Payment Gateway

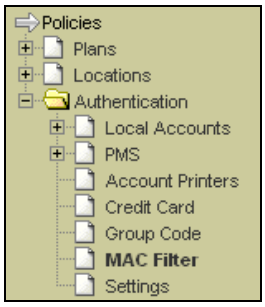
1. **Payment Gateway**
2. **Transaction Type –** Choose “Test Mode” if you are testing.
3. **Merchant ID**
4. **Transaction Key**
5. **Currency** – Currency to be used in the transaction

Depending on the selected payment gateway, the fields will change accordingly and that depends what functions are made available by the service provider.

Details of credit card are explained in Appendix G.

2.6 MAC Filter

Use this as a MAC-based firewall to block or allow devices.



To access the option:

1. Click on **Authentication**.
2. Click on **MAC Filter**.

You can now select the **Blocked MAC Addresses** tab to add devices that you want to block. Error pages are explained in details in Appendix F.

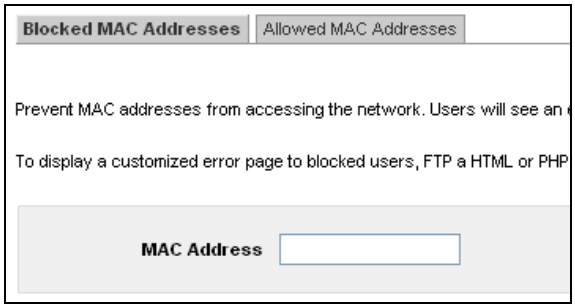
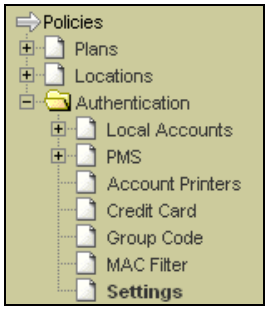

Blocked MAC Addresses
Allowed MAC Addresses
Prevent MAC addresses from accessing the network. Users will see an
To display a customized error page to blocked users, FTP a HTML or PHP
MAC Address

Figure 2-21 Blocked MAC

Conversely, select the **Allowed MAC Addresses** tab to add devices that are allowed access to the network without login.

2.7 Global Settings

Here you can configure the global settings that will apply to all accounts.



To access the option:

1. Click on **Authentication**.
2. Click on **Settings**.

The following sections are available:

1. **Auto-Logout** – This tells the system to logout users that have been detected to be inactive for a period of time.

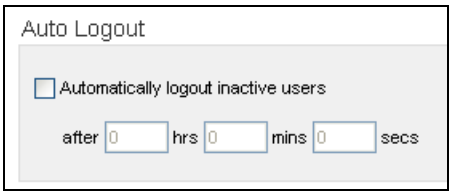


Figure 2-22 Auto-Logout

Chapter 3

LAN NETWORK SETTINGS

3.1 Overview

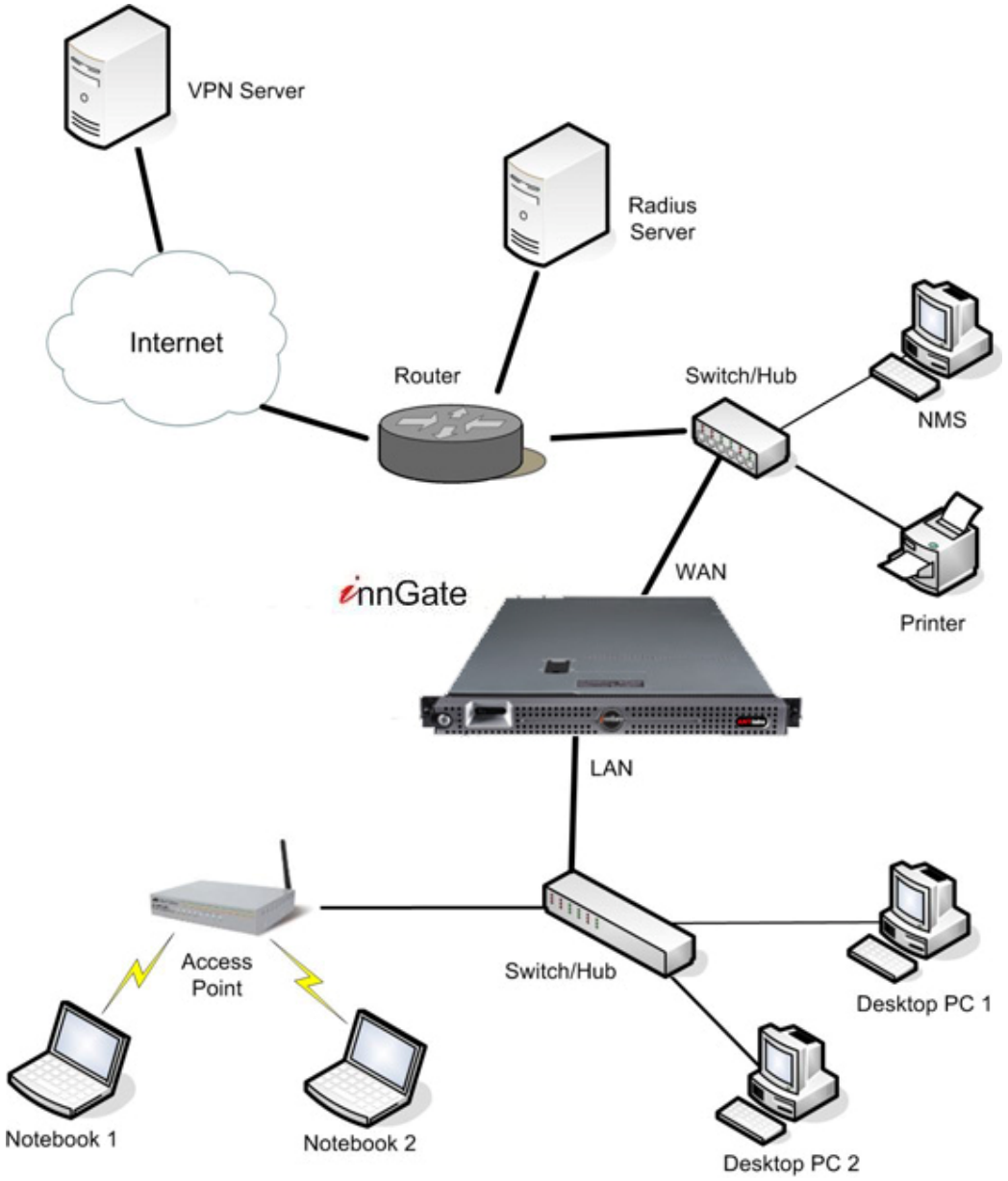


Figure 3-1 Example Network Setup

This chapter covers the basic LAN network settings that allow you to configure how the InnGate will manage the downstream network:

1. **DHCP Setup** – See Section 3.2
2. **Routed Network Setup** – See Section 3.3.
3. **Walled Garden Setup** – See Section 3.4.
4. **Network Devices Setup** – See Section 3.5.
5. **Device Detection Setup** – See Section 3.6.
6. **ARP Setup** – See Section 3.7.

3.2 DHCP Setup

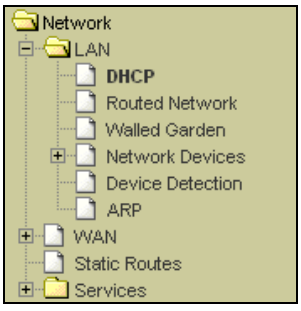
The InnGate can be configured as either a DHCP server, DHCP relay or to operate without any DHCP services enabled. Each of these modes is described in the following sections:

1. **Configuring DHCP Server Mode** – See Section 3.2.1.
2. **Configuring DHCP Relay Mode** – See Section 3.2.2.

3.2.1 Configuring DHCP Server Mode

When the InnGate is setup in DHCP Server mode, downstream clients will be assigned IP addresses from one of two DHCP scopes:

1. **Default Scope** – The pool of IP addresses that are assigned to clients by default. Traffic from these clients can be either routed upstream or via Network Address and Port Translation (NAPT). See Section 3.2.1.1.
2. **User Provision Routed Scope** – The pool of IP addresses that are assigned to clients on request. Traffic from these clients is always routed upstream. See Section 3.2.1.2.



To setup the DHCP Server:

1. Click on **LAN**.
2. Click on **DHCP**.

Figure 3-2 shows part of the DHCP **Settings** configuration page.

Select the **DHCP Server** option.

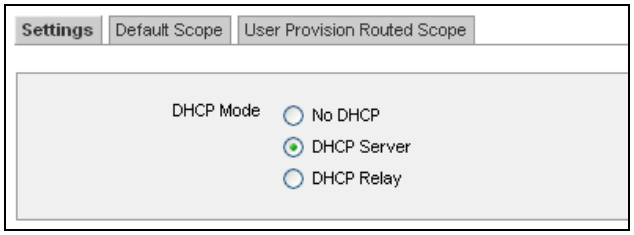


Figure 3-2 DHCP Mode

Figure 3-3 shows the configuration settings for the **Default Scope**. The fields are described as follows:

1. **Default Lease** – The amount of time before a lease on an IP address expires and is applied when the client does not specifically request the lease duration.

2. **Max Lease** – Specify the maximum lease duration that can be requested from DHCP clients.

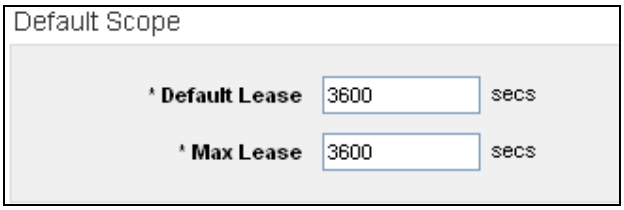


Figure 3-3 Default Scope Settings

Figure 3-4 shows the configuration settings for the **User Provision Routed Scope**. The fields are the same as for the Default Scope.

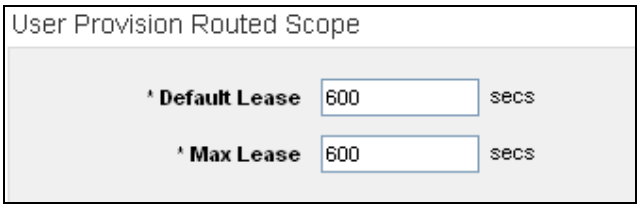


Figure 3-4 User Provision Routed Scope Settings

Click Save to commit the changes.

After saving the **Settings** for DHCP Server mode, additional option tabs called **Default Scope** and **User Provision Routed Scope** will be available.

Next we proceed to define the IP addresses for the different scopes:

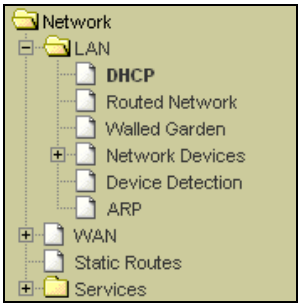
1. **Setting up the Default Scope** – See Section 3.2.1.1.

2. **Setting up the User Provision Routed Scope** – See Section 3.2.1.2.

When the client first connects on the downstream LAN, the InnGate will assign an IP address from the Default Scope to the client via DHCP initially. The client may be allowed to request for a routed IP address from the User Provision Routed Scope.

⚠ The propagation of this new routable IP will only occur when the client seeks to renew the DHCP lease, which is half of the lease expiry time. Alternatively, the client can force an immediate change in IP by releasing and renewing its IP address.

3.2.1.1 Setting up the Default Scope



To setup the Default Scope:

1. Click on **LAN**.

2. Click on **DHCP**.

Select the **Default Scope** tab as shown in Figure 3-5.

A list of IP address ranges will be presented. Click on an entry to modify it or click Add to create one.

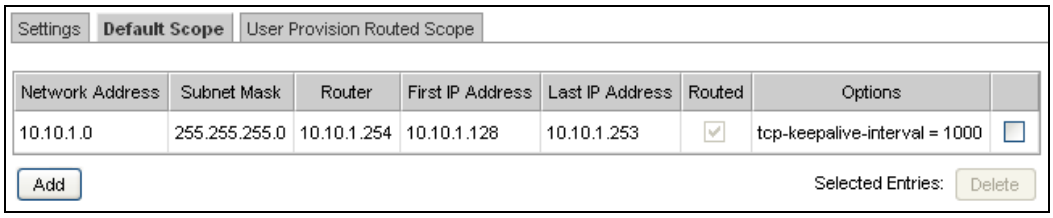


Figure 3-5 Default Scope IP Addresses

⚠ Ensure that there is no overlap of the IP address ranges between the Default Scope and User Provision Routed Scope.

Figure 3-6 shows the Default Scope configuration page.

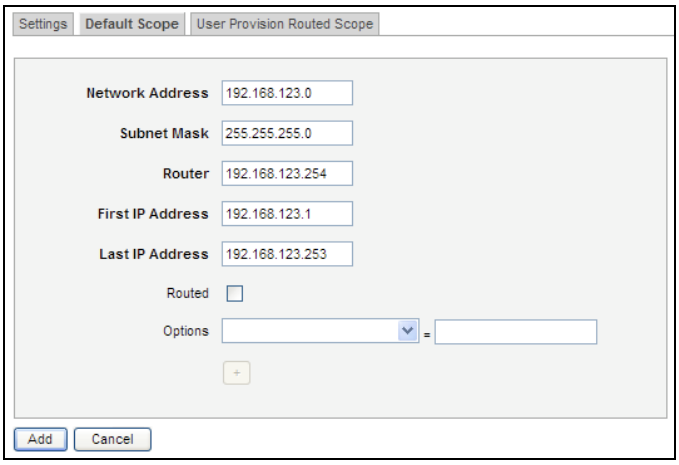


Figure 3-6 Defining an IP address pool

The fields are explained as follows:

1. **Network Address** – The network from which IP host addresses will be assigned to downstream clients.

2. **Subnet Mask** – Subnet mask for the Network IP Address.

3. **Router** – The IP address of the router entry to be assigned to downstream clients. This entry will be excluded from the address range that can be assigned (which is defined by the **First** and **Last IP Address** fields).

4. **First IP Address** – The first IP address of the IP range to be assigned.

   ⚠ The First and Last IP Addresses must fall within the subnet defined above.

5. **Last IP Address** – The last IP address of the IP range to be assigned.

6. **Routed** – When enabled, the InnGate will not perform NAPT for the packets from clients assigned these IP addresses. Instead the packets are routed upstream.

   ⚠ While you can configure one IP address pool to be routed and another to be non-routed, it is considered an unusual practice and is not recommended. This is because the LAN client in the Default Scope

may or may not get a routed IP address as the InnGate will assign these addresses in no particular order.

7. **Options** – Figure 3-7 shows the interface for configuring the DHCP options that are sent to the client.

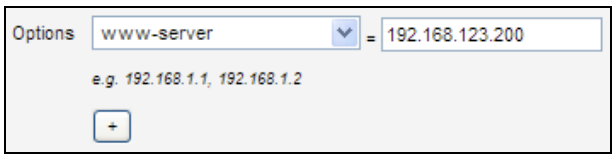


Figure 3-7 Adding DHCP options

Select the DHCP option from the drop down list and enter the value for that option. Click + to add the option to the list as shown in Figure 3-8.

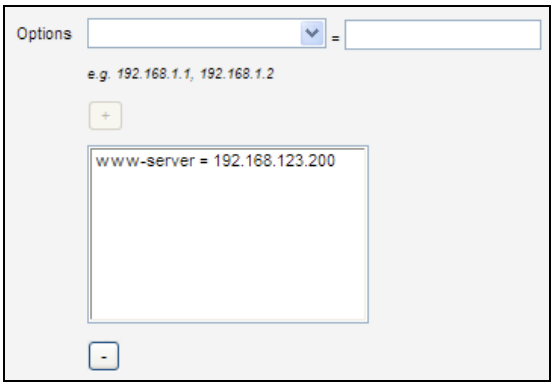
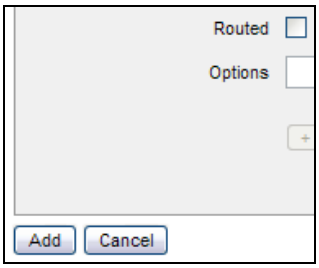


Figure 3-8 DHCP options

To delete any option from the list, select the entry and click -.

To commit the Default Scope entry, click on the Add button (or Save for modifications).



3.2.1.2 Setting up the User Provision Routed Scope

Downstream clients may be allowed to request for a routed IP address when logging on to the network (see Section 3.2.1.1) by selecting the "**Obtain routable IP address**" option. These IP addresses come from the User Provision Routed Scope.

It is quite common for the User Provision Routed Scope to be configured as set of public IP addresses although private addresses are also accepted. Section 3.2.1.2 discusses the common scenarios where public IP addresses may be needed by the LAN clients.

⚠ For clients without DHCP enabled or configured with a static IP, the InnGate will not be able to assign a routed IP to it.

Figure 3-9 Routed IP addresses

Some applications such as VPN and video conferencing require that the clients be assigned a public IP address and the User Provision Routed Scope with a set of public IP addresses can be used to accommodate such scenarios:

1. **Connecting to Virtual Private Networks** – Often, clients on the LAN may need to connect to a VPN server, for example, to access a corporate enterprise network securely from a remote location. This is a common requirement of business travelers or telecommuters.

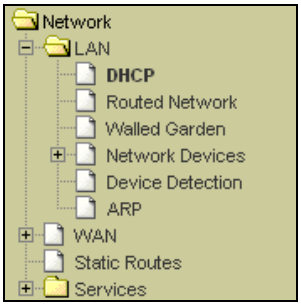
   Although quite uncommon, some VPN applications do not always work with devices performing NAPT between the VPN server and the connecting client. This is because the process of network address translation modifies the IP header (and the TCP port) thus violating the IPSec checksum integrity used by some VPN and the resulting packets will be dropped by the VPN server.

   As such, clients that need access to VPN services will need to select the public IP option. Once the InnGate assigns a public IP address to the client, packets sent by the client through the InnGate will not be

subject to NAPT but instead routed on the upstream and therefore "VPN friendly".

2. **Video Conferencing and Other Applications** – Another common use of public IP is when a client on the downstream sets up a video conferencing server to conduct a video conference. The participants of the conference could be connecting from a remote location from the upstream and will therefore need to configure its video conferencing software to connect to a public IP address (of the server).

   Other similar applications that also require a public IP may include multiplayer game servers, FTP servers, etc. In all these scenarios, the downstream user will need to select public IP upon login in order to be assigned a valid routable IP address to allow for clients from the WAN to connect to it.



To setup the User Provision Routed Scope:

1. Click on **LAN**.
2. Click on **DHCP**.

Select the **User Provision Routed Scope** tab as shown in Figure 3-10.

Any existing entries will be displayed. Click on an entry to modify it or click Add to create one.

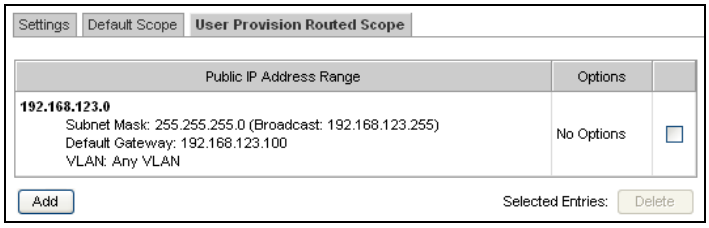


Figure 3-10 User Provision Routed Scope Entries

Figure 3-11 shows the configuration interface to define the User Provision Routed Scope.

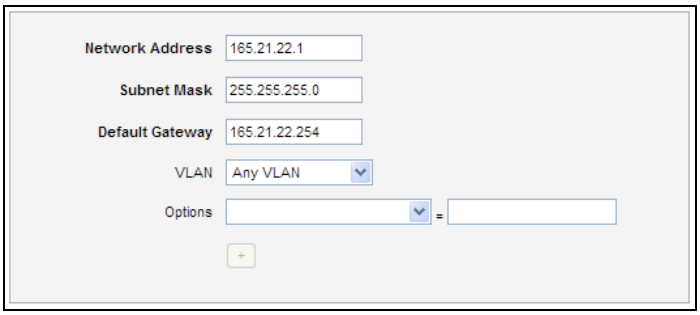


Figure 3-11 User Provision Routed Scope

The fields are described as follows:

1. **Network IP Address** – The network from which IP host addresses will be assigned to downstream clients.

2. **Subnet Mask** – Subnet mask for the Network IP Address.

3. **Default Gateway** – Clients will be configured with the default gateway specified here.

4. **VLAN** – Restricts this scope to be applied to a particular VLAN only.

5. **Options** – Figure 3-12 shows the interface for configuring the DHCP options that are sent to the client.

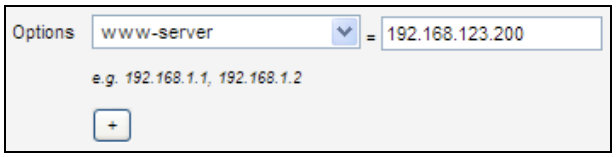


Figure 3-12 Adding DHCP options

Select the DHCP option from the drop down list and enter the value for that option. Click + to add the option to the list as shown in Figure 3-13.

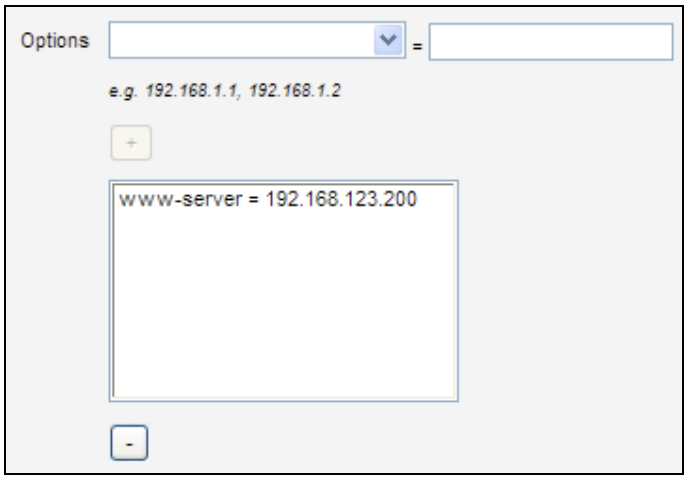
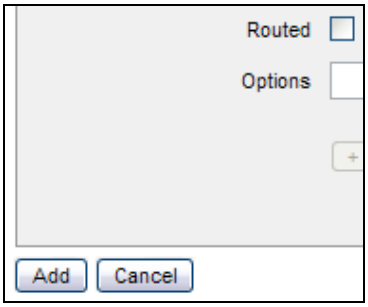


Figure 3-13 DHCP options

To delete any option from the list, select the entry and click -.

To commit the User Provision Routed Scope entry, click on the Add button (or Save for modifications).



⚠ The InnGate will perform a proxy ARP on the upstream when it encounters user provisioned routed IP addresses that have been assigned to its downstream devices. The InnGate will not proxy ARP for addresses that have not been assigned. Thus when defining the routing table of the router on the WAN segment, traffic destined for the IP addresses in the User Provisioned Routed Scope should be sent to the WAN subnet rather than directly to the InnGate's WAN IP address.

There are two additional configuration options which are accessible when you select an existing entry (from the list shown in Figure 3-14) to modify.

The additional interface options are shown in Figure 3-14:

1. **Disabled IP Addresses** – IP addresses that will not be assigned to the DHCP clients. This feature is commonly used to exclude the IP addresses of statically configured “permanent” network devices such as routers, printers, etc.

2. **Reserved IP Addresses** – Used to map an IP address to a particular MAC address. When the system detects that a DHCP client's MAC address is in this list, it will assign the corresponding IP address to it.

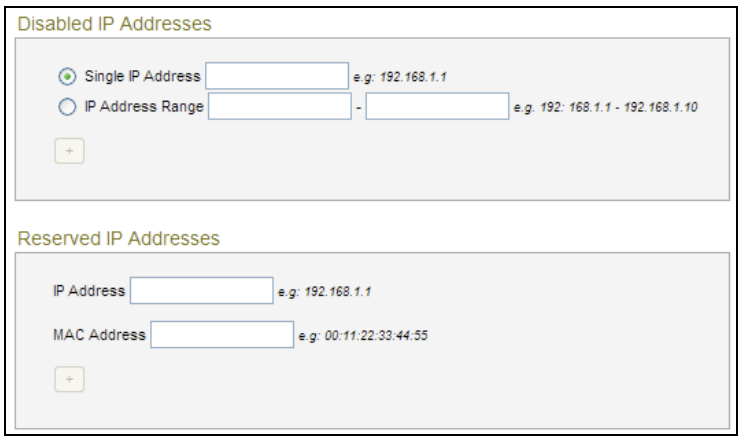


Figure 3-14 Additional DHCP configuration options

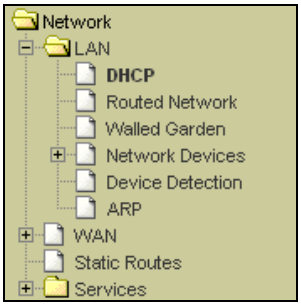
3.2.2 Configuring DHCP Relay Mode

With the DHCP relay feature, the InnGate can relay DHCP requests and responses between the downstream clients and a DHCP server on the upstream.

Configuring the InnGate for DHCP Relay is a two step process:

1. Configuring the InnGate to interface with the external DHCP server.

2. Setting up the InnGate so that the IP addresses assigned by the external DHCP server are not subject to Network Address and Port Translation (NAPT) and therefore defined in the Routed Network (see Section 3.3).



To setup DHCP Relay:

1. Click on **LAN**.

2. Click on **DHCP**.

Figure 3-15 shows part of the DHCP **Settings** configuration page.

Select the **DHCP Relay** option.

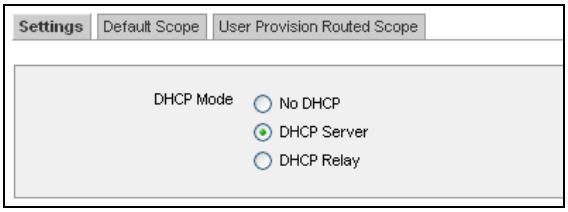


Figure 3-15 DHCP Mode

Figure 3-16 shows the configuration settings for the **DHCP Relay**. The fields are described as follows:

1. **Primary Server** – The primary DHCP server that the InnGate will relay to.

2. **Secondary Server** – Alternate DHCP server.

   ⚠ The InnGate will forward DHCP requests to both servers but will only acknowledge and use the first response it receives, ignoring the other reply.

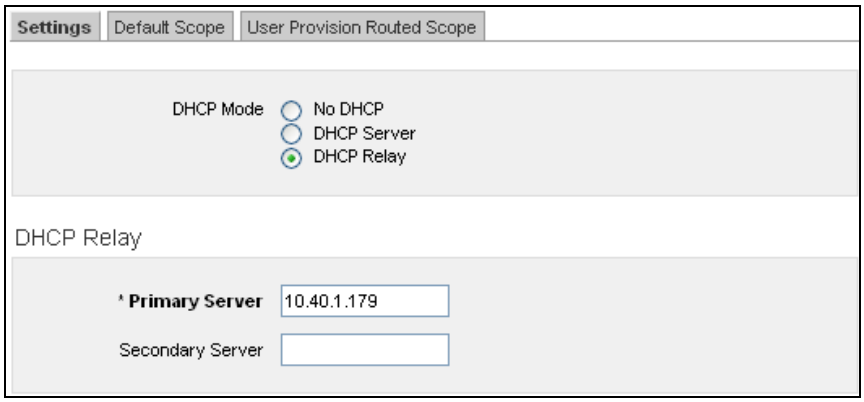


Figure 3-16 DHCP Relay Settings

Click Save to commit the changes.

⚠ You will need to configure the DHCP range in the Routed Network so that the InnGate does not perform Network Address and Port Translation (NAPT) for the externally assigned IP addresses. See Section 3.3.

3.2.2.1 Relay Agent Mappings

After saving the **Settings** for DHCP Relay mode (see Section 3.2.2), an additional option tab called **Agent Mapping** will be available as shown in Figure 3-17.

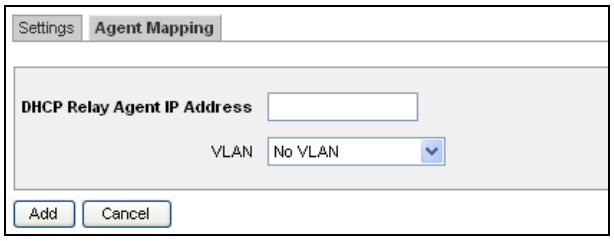


Figure 3-17 DHCP Relay Agent Mapping

This feature allows different IP address pools to be allocated to clients belonging to different VLANs when in DHCP Relay mode.

For example, an administrator may wish to allocate the IP addresses in the subnet 192.168.123.0/28 to the clients on the "Office VLAN" while the clients on the "Meeting Room VLAN" will get addresses from the 192.168.123.128/28 subnet.

This is done by configuring the InnGate to use a different DHCP Relay Agent IP address for each VLAN when it sends a DHCP request on behalf of the downstream client. In the case of the above example, the InnGate can be configured to use the IP address 10.10.10.1 when sending DHCP requests for any of the clients on the "office VLAN".

You can then configure the DHCP server to respond with the desired IP address range based on the DHCP Relay Agent IP address it receives.

The fields are described as follows:

1. **DHCP Relay Agent IP Address** – The IP address that the InnGate will use when relaying DHCP requests from downstream clients.

2. **VLAN** – The VLAN for which the **Relay Agent IP Address** is applicable.

Click Add to confirm the entry (or Save for modifications).

3.3 Routed Network Setup

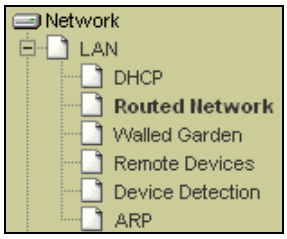
Using this function, you can configure IP addresses that will always be routed on the upstream whenever the InnGate encounters network packets which contain these addresses in either the source or destination IP.

There are some circumstances in which this would be useful:

1. When operating in DHCP Relay mode (see Section 3.2.2), IP addresses are assigned to downstream clients from an external DHCP Server. In

this case, InnGate must not perform NAPT for these clients and therefore the DHCP range is defined in the Routed Network.

2. The InnGate may be required to route packets from downstream clients to resources on the upstream that are within the intranet (such as intranet portals) but perform NAPT for Internet traffic. In this case, the intranet resources will be defined in the Routed Network.



To setup Routed Networks:

1. Click on **LAN**.
2. Click on **Routed Network**.

Any existing entries will be displayed (see Figure 3-18). Click on an entry to modify it or click Add to create one.

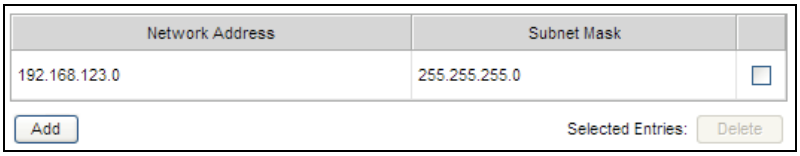


Figure 3-18 List of Routed Networks

Figure 3-19 shows the interface for defining a Routed Network:

1. **Network Address** – The network within which the IP addresses will be routed.

2. **Subnet Mask** – The subnet mask for the Network IP Address.

   ⚠ To define a specific host IP address, use 255.255.255.255 for the subnet mask.

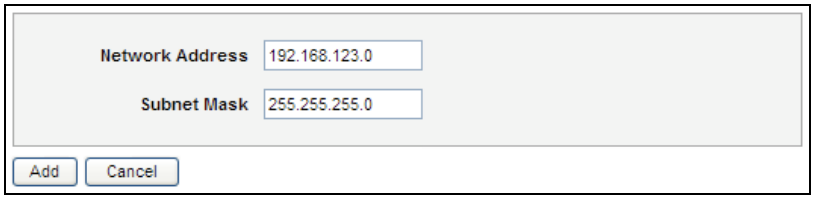


Figure 3-19 Defining a Routed Network

In this example, the InnGate will route packets originating from or destined for the network identified by the network address 192.168.123.0 and subnet mask 255.255.255.0.

Click Add to confirm the entry (or Save for modifications).

3.4 Walled Garden Setup

This feature allows you to configure HTTP URLs, HTTPS Domain and IP Addresses that the InnGate will allow downstream clients to access before authentication.

A common example of using this feature is in a charged Internet usage environment where you need to allow the user to access a credit card payment portal to complete the purchase transaction before he has logged in. The payment portal will be defined in the Walled Garden so that even though the user is not logged in and therefore does not have Internet access, he can still access the portal.

There are three different types of definitions in the Walled Garden:

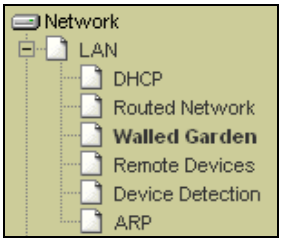
1. **Define HTTP URLs** – See Section 3.4.1.

2. **Define HTTPS Domains** – See Section 3.4.2.

3. **Define IP Addresses** – See Section 3.4.3.

3.4.1 Define HTTP URLs

You can define a whitelist of URLs that the InnGate will allow non-logged in users to access.



To define HTTP URLs in the Walled Garden:

1. Click on **LAN**.
2. Click on **Walled Garden**.

Select the **HTTP URLs** tab as shown in Figure 3-20.

Any existing entries will be displayed. Click on an entry to modify it or click Add to create one.

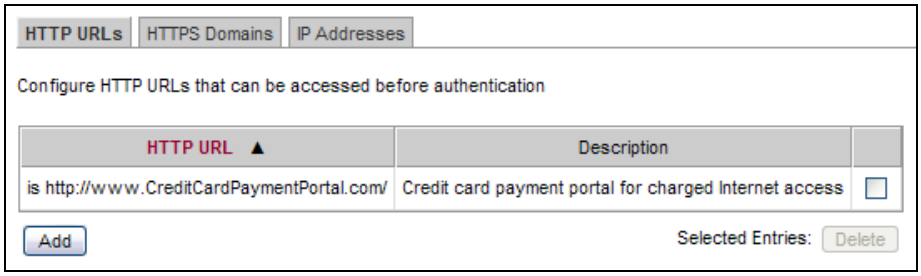


Figure 3-20 Whitelist of HTTP URLs

Figure 3-21 shows the interface for defining a HTTP URL in the Walled Garden.

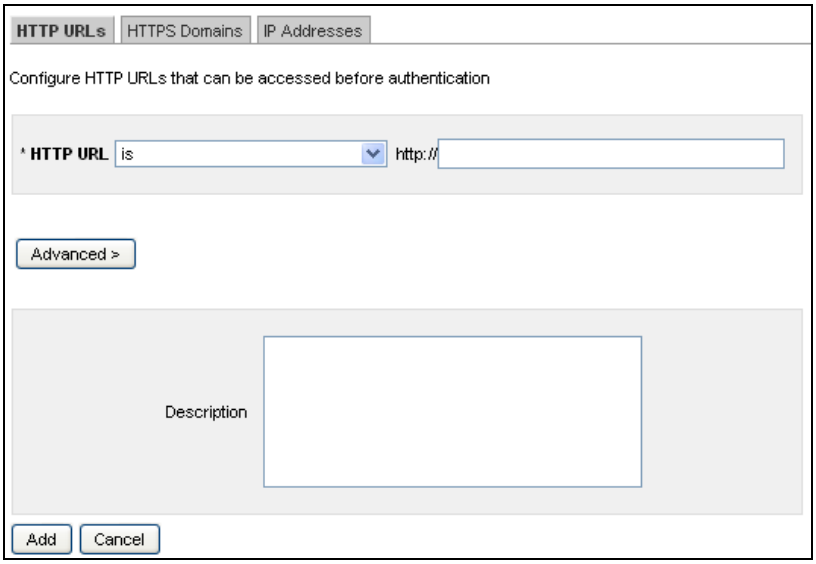


Figure 3-21 Define HTTP URL in the Walled Garden

The fields are described as follows:

1. **HTTP URL** –

Condition	Value to Match	Match Result
begins with	**http://ftp.**	✓ **http://ftp.antlabs.com** × **http://ftpezxcess.com.sg**
is	**http://www.antlabs.com**	✓ **http://www.antlabs.com** × **http://www.antlabs.com.sg**
ends with	**.com**	✓ **http://www.antlabs.com** × **http://ftpezxcess.com.sg**
contains	**antlabs**	✓ **http://ftp.antlabs.com** ✓ **http://www.antlabs.com**
matches the regular expression	**See Appendix B**	
is the SmartURL™		

2. **http://** – Allow access to the URL that matches the condition.

3. **Description** – A description for the entry.

Click Advanced > to set advanced options for the Walled Garden entry. Figure 3-22 shows the interface for defining advanced options for HTTP URLs in the Walled Garden.

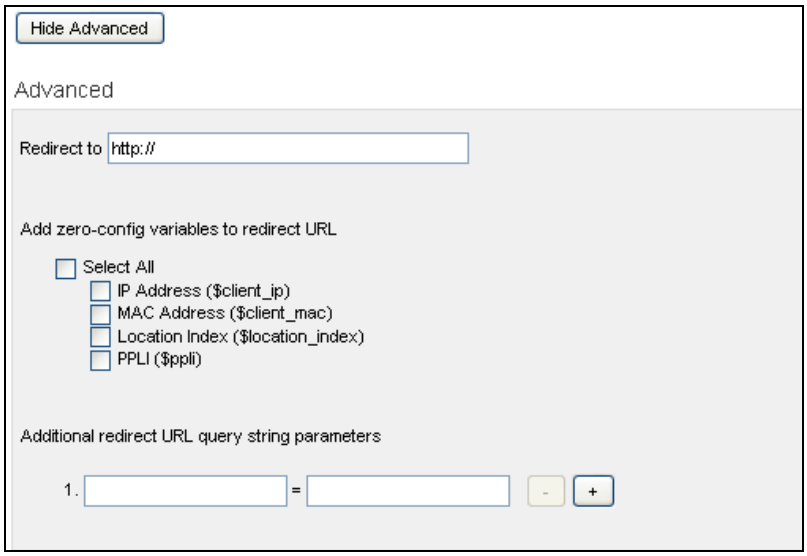


Figure 3-22 Advanced options in the HTTP URLs Walled Garden

The fields are described as follows:

1. **Redirect to** – Redirect the user to the URL defined here if the HTTP URL condition matches

2. **Add zero-config variables to redirect URL** – Select any of the variables to be added to the redirected URL query string.
   a. If "IP Address" is selected, the name in the parenthesis will be added to the redirect URL, e.g. <URL>?client_ip=<IP Address>

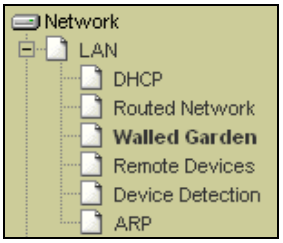
3. Additional redirect URL query string parameters – Set any other variables to be added to the redirected URL query string.
   a. If "name = value" is input, the redirect URL will become <URL>?name=value
   b. Click + to add additional URL query string parameters. If there are more than 1 parameter added, the redirect URL will become <URL>?name=value&name2=value2...
   c. Click - to remove any unwanted parameters

Click Add to confirm the entry (or Save for modifications).

3.4.2 Define HTTPS Domains

Some clients may be configured to use a web proxy server and when the client accesses a HTTPS website, the proxy protocol will require that the HTTPS Domain Name be defined in the Walled Garden.

⚠ If the client is not using a proxy server, define the domain under **IP Addresses** instead. However, if client proxy settings are not deterministic, then you will need to create both entries.



To define HTTP Domains in the Walled Garden:

1. Click on **LAN**.
2. Click on **Walled Garden**.

Select the **HTTP Domains** tab as shown in Figure 3-23.

Any existing entries will be displayed. Click on an entry to modify it or click Add to create one.

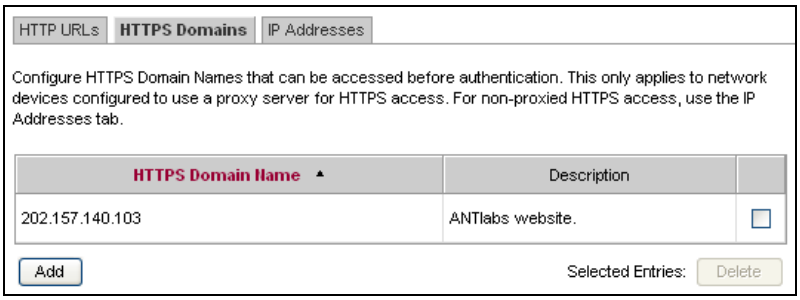

HTTP URLs
HTTPS Domains
IP Addresses
Configure HTTPS Domain Names that can be accessed before authentication. This only applies to network devices configured to use a proxy server for HTTPS access. For non-proxied HTTPS access, use the IP Addresses tab.
HTTPS Domain Name
Description
202.157.140.103
ANTlabs website.
Add
Selected Entries:
Delete

Figure 3-23 Whitelist of HTTPS Domains

Figure 3-24 shows the HTTPS Domain Definition page with the following fields:

1. **HTTPS Domain Name** – IP address of the HTTPS web server.
2. **Description** – A description for this entry.

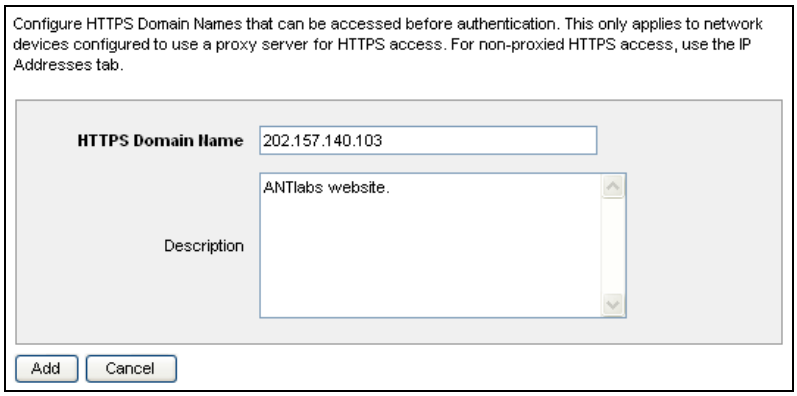
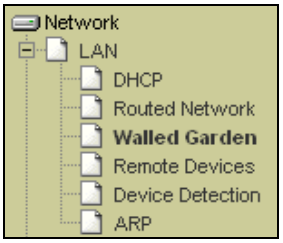

Configure HTTPS Domain Names that can be accessed before authentication. This only applies to network devices configured to use a proxy server for HTTPS access. For non-proxied HTTPS access, use the IP Addresses tab.
HTTPS Domain Name
202.157.140.103
Description
ANTlabs website.
Add
Cancel

Figure 3-24 HTTPS Domain Definition

3.4.3 Define IP Addresses

This feature allows you to filter packets that downstream clients are allowed to send before they are logged in.



To define IP addresses in the Walled Garden:

1. Click on **LAN**.
2. Click on **Walled Garden**.

Select the **IP Addresses** tab as shown in Figure 3-25.

Any existing entries will be displayed. Click on an entry to modify it or click Add to create one.

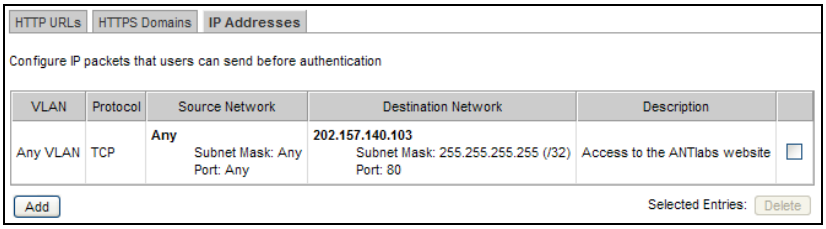


Figure 3-25 Whitelist of IP addresses

Figure 3-26 shows the interface for defining IP addresses in the Walled Garden.

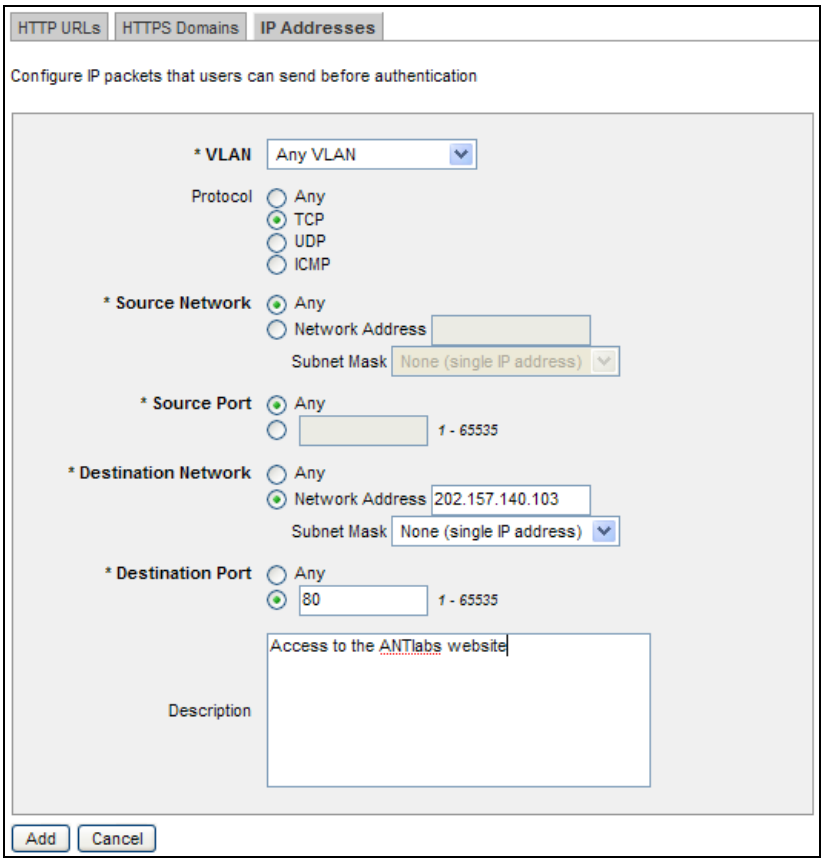


Figure 3-26 Define IP packets allowed before login

The fields are described as follows:

1. **VLAN** – Packets from this VLAN is allowed.

2. **Protocol** – Specify the protocol allowed.

3. **Source Network** – Packets whose source field matches the criteria here are allowed.

4. **Source Port** – Packets whose source port field matches the entry here are allowed.

5. **Destination Network** – Packets whose destination field matches the criteria here are allowed.

   ⚠ If you are creating this IP Address Walled Garden entry as part of the HTTPS Domain requirements (see Section 3.4.2) this will be the IP of the web server that will handle the HTTPS traffic.

6. **Destination Port** – Packets whose destination port field matches the entry here are allowed.

⚠ If you are creating this IP Address Walled Garden entry as part of the HTTPS Domain requirements (see Section 3.4.2) then the port number here should be 443. This is the standard port for HTTPS traffic.

7. **Description** – A description for the entry.

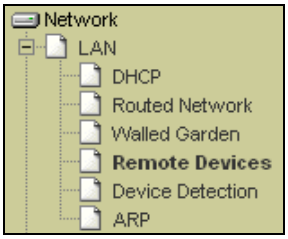
Click Add to confirm the entry (or Save for modifications).

3.5 Network Devices Setup

Sometimes downstream devices may need to be accessed by clients on the upstream. For example, a network administrator may use an NMS on the upstream to monitor wireless access points on the downstream (see Figure 3-1).

Such devices are registered as **Network Devices**. Subsequently, whenever an upstream device sends packets to a downstream Network Device, the InnGate will perform a proxy ARP on the WAN interface on behalf of the Network Device, receive the packets, and then forward to it.

⚠ Network Devices often need to communicate back to the sender. Unlike a downstream user who will initiate a browser session to authenticate themselves, devices such as access points cannot do this to gain network access. As such, the InnGate comes preloaded with a Plan that is applied to registered Remote Devices.



To setup Remote Devices:

1. Click on **LAN**.
2. Click on **Remote Devices**.

Any existing entries will be displayed (see Figure 3-25). Click on an entry to modify it or click Add to create one.

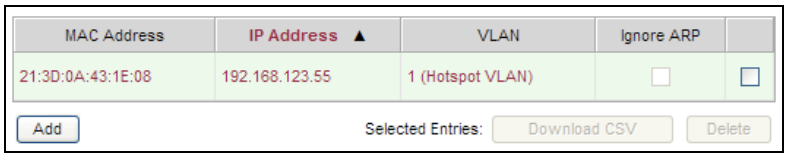


Figure 3-27 List of Network Devices

Figure 3-28 shows the interface for registering a Remote Device:

1. **MAC Address** – MAC address of the device to be registered. The format of the MAC Address is "xx:xx:xx:xx:xx:xx".

2. **IP Address** – IP address of the device to be registered.

3. **VLAN** – VLAN that the device to be registered is on.

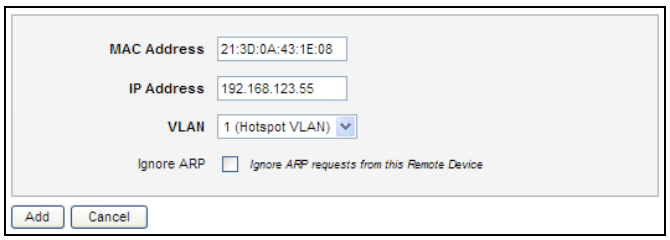


Figure 3-28 Network Device Configuration

Click Add to confirm the entry.

3.5.1 Port Binding

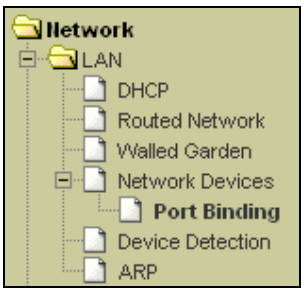
In a typical deployment, an NMS is used to monitor the key network components such as routers and access points. The NMS is normally run from a remote location and may have problems accessing devices that are found on the downstream such access points.

This is because downstream network is usually a private network that is not visible to the upstream because the InnGate performs NAPT. In such cases, upstream users will only see the WAN IP of the InnGate and not the individual downstream hosts. So there will be no way for an upstream user to connect to a particular downstream device.

Port Binding allows you to configure a port forwarding service which allows incoming traffic from the upstream to reach downstream devices.

Port Binding allows you to assign a Port Number on the InnGate's WAN interface so that a user connecting to the InnGate's WAN IP + Port Number will actually have their traffic forwarded to the downstream service. The InnGate thus acts as a port forwarding proxy for incoming upstream traffic.

Port Binding can also be used as a means to conserve public IP addresses; as opposed to assigning a public IP for each downstream service host.



To access the option:

1. Click on **LAN**.
2. Click on **Network Devices**.
3. Click on **Port Binding**.

Figure 3-29 shows the Port Binding Rules setting page. This GUI is used to setup a port on the InnGate's WAN interface that upstream clients can connect to in order to reach a particular downstream host.

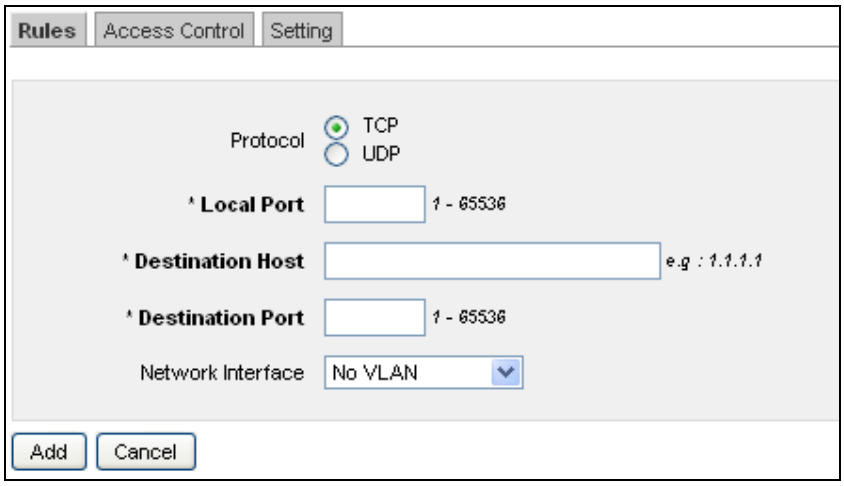


Figure 3-29 Port Binding Rules

The fields are described as follows:

1. **Protocol** – Specify the protocol that is allowed over the proxied connection.
2. **Local Port** – This is the port on the InnGate that the upstream client will connect to in order to connect to the downstream device.

   ⚠ Do not use ports 61000 to 65096 as these are reserved by InnGate for IP masquerading.

3. **Destination Host** – IP address of the downstream host that traffic will be forwarded to. You can use CIDR notation to specify the subnet mask. e.g. 10.2.3.11/24
4. **Destination Port** – The IP port of the downstream host that traffic will be forwarded to.

5. **Network Interface** – Specify if the traffic should be forwarded to a specific VLAN on the downstream where the host resides.

Click Add to confirm the entry.

After configuring the proxy rule, you can further restrict access by creating access control rules that determine the action to take when incoming traffic that matches certain criteria is detected. Figure 3-30 shows the Port Binding Access Control page.

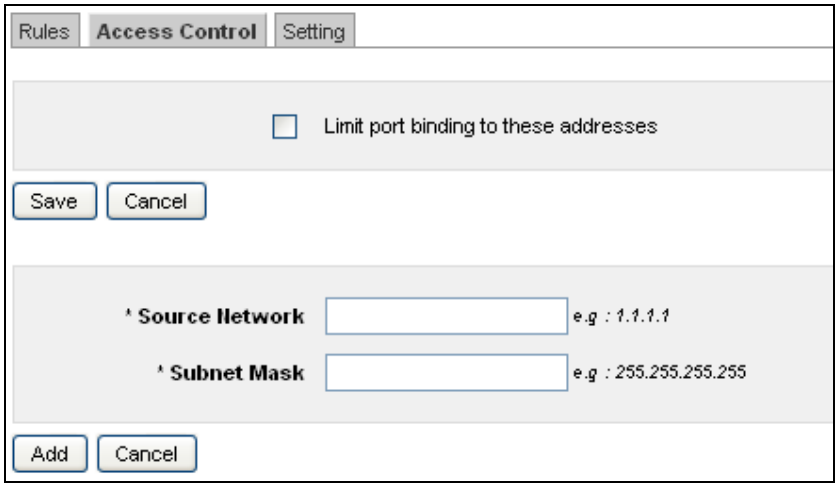


Figure 3-30 Port Binding Access Control

The fields are described as follows:

1. **Limit port binding to these addresses –** To limit only allowed addresses to use port binding.

2. **Source Network** – Matches the value of the source IP address field in the incoming network packet.

3. **Subnet Mask**

Click Add to confirm the entry.

After you have configured the port forwarding and access control rules, you can also to specify the settings that determine the general behavior of the Port Binding system as shown in Figure 3-31.

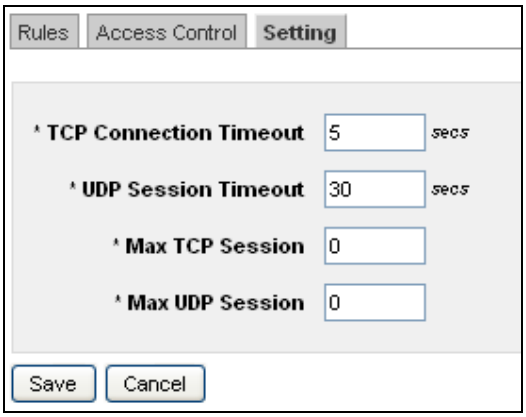


Figure 3-31 Port Binding Setting

The fields are described as follows:

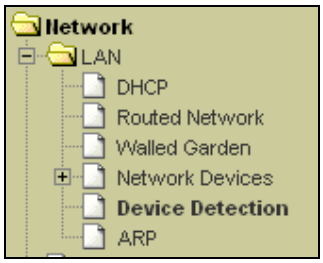
1. **TCP Connection Timeout** – Timeout for TCP connection attempts.
2. **UDP Session Timeout** – Timeout for UDP connection attempts.
3. **Max TCP Session** – Maximum number of TCP sessions allowed.
4. **Max UDP Session** – Maximum number of UDP sessions allowed.

Click Save Changes to commit the changes.

3.6 Device Detection Setup

The InnGate sends ARP requests (ARP probe) on the downstream to determine whether a remote device is still on the LAN or has physically disconnected.

The device detection feature is activated by default and you may make changes to the respective fields to suit your network environment.



To configure the Device Detection settings:

1. Click on **LAN**.
2. Click on **Device Detection**.

Figure 3-32 shows the Device Detection settings page.

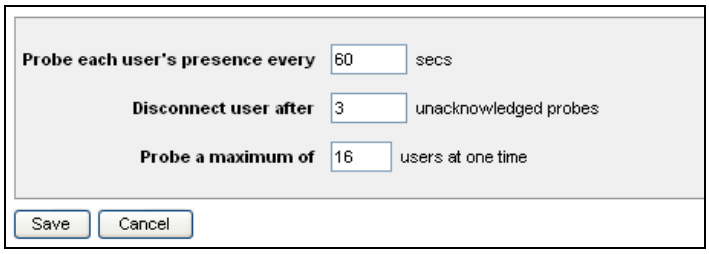


Figure 3-32 Device Detection Settings

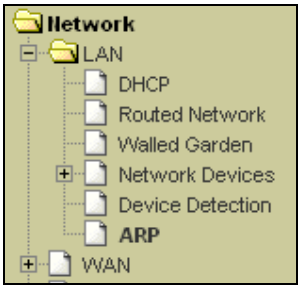
The fields are described as follows:

1. **Probe each user's presence...** – Interval between probes.
2. **Disconnect user after...** – Specify the number of unacknowledged probes before the user is disconnected.
3. **Probe a maximum of...** – Select a value between 0 – 45 depending on the network requirements.

Click Save to confirm the changes.

3.7 ARP Setup

You can configure how the InnGate will manage ARP requests and responses.



To configure the ARP settings:

1. Click on **LAN**.
2. Click on **ARP**.

Figure 3-33 shows the ARP Settings configuration page.

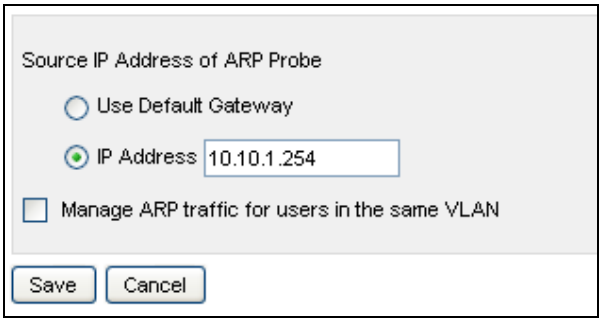


Figure 3-33 ARP Settings

The fields are described as follows:

1. **Source IP Address of ARP Probe**:

    a. **Use Default Gateway** – Uses the IP address of the Default Gateway defined under the WAN profile (see Section 4.2) as the source address of the ARP probes that it sends out.

    b. **IP Address** – Depending on the network setup, the downstream subnet may not be the same as the subnet of the Default Gateway and some devices are known to ignore ARP requests that are not from their own subnet. If you encounter such cases, you can configure the Source IP Address of the ARP probe here.

2. **Manage ARP traffic for users in the same VLAN** – This is normally unselected to allow users within the same VLAN to communicate directly with each other. If the checkbox is selected, the InnGate will respond to clients' ARP requests in an attempt to manage their communications.

Click to confirm the changes.

Chapter 4

WAN NETWORK SETTINGS

4.1 Overview

You can configure the following under the WAN Settings:

1. **WAN Setup** – See Section 4.2.

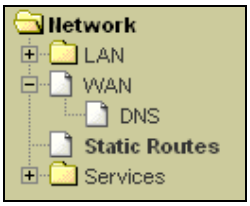
2. **DNS Setup** – This was previously covered in *Chapter 1: GETTING STARTED* under *Section 1.3.3: Configuring the Domain Name Server*.

4.2 WAN Setup

Like any other device connecting to a network, the InnGate's network settings such as its IP address on the upstream must be configured. The WAN setup interface allows you to do this:

1. Configuring the WAN interface was previously covered in *Chapter 1: GETTING STARTED* under *Section 1.3.2: Configuring the WAN Interface*.

4.2.1 Defining a Static Route



To setup a Static Route for a Service Provider:

1. Click on **Static Routes**.

Any existing entries will be displayed (see Figure 4-1). Click on an entry to modify it or click Add to create one.

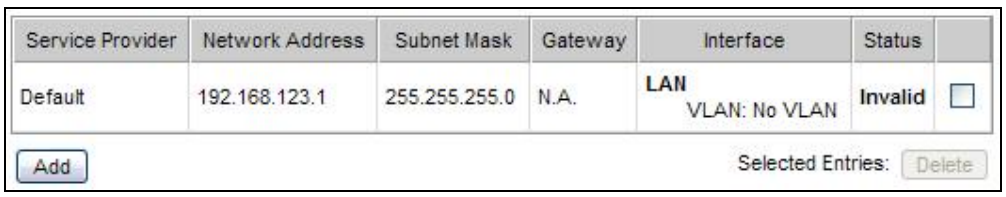


Figure 4-1 List of Static Routes

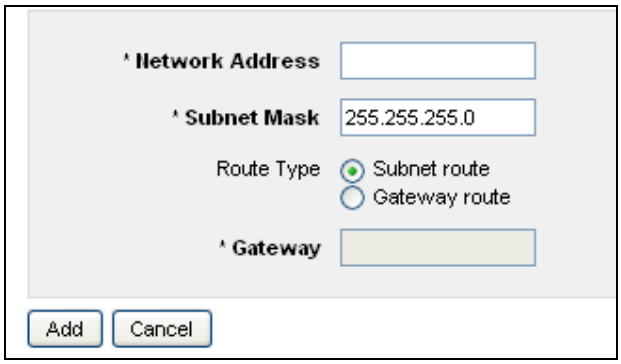


Figure 4-2 Defining Static Routes

Figure 4-2 shows the interface for defining a static route to a previously defined Service Provider:

1. **Network Address** – Specify the Network Address for this Static Route
2. **Subnet Mask** – Subnet Mask for the Network Address
3. **Route Type** – Indicate if this entry is a Subnet or Gateway route

Chapter 5

NETWORK SERVICES SETTINGS

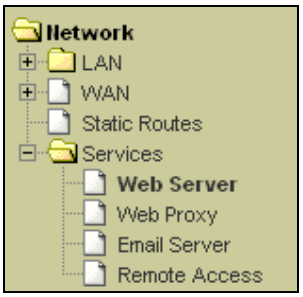
5.1 Overview

You can configure the following under the Services option:

1. **Web Server** – See Section 5.2.
2. **Web Proxy** – See Section 5.3.
3. **Email Server** – See Section 5.4.
4. **Remote Access –** See Section 5.5.

5.2 Web Server

This email address is displayed to users in the Web Server error pages.



To set the Web Server admin email:

1. Click on **Services**.
2. Click on **Web Server**.

Enter the email address in the **Display Email** field as shown in Figure 5-1.

Click Save to confirm the changes.

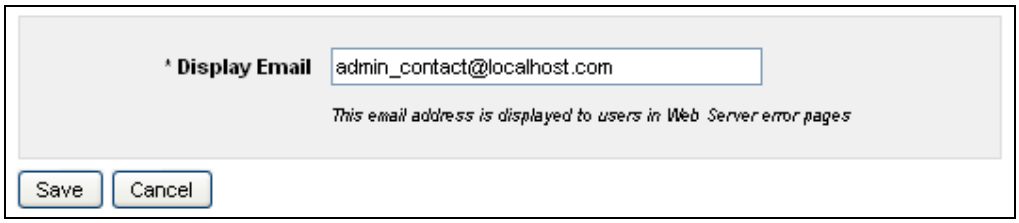
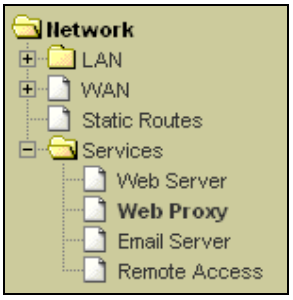


Figure 5-1 Web Server Admin Contact

5.3 Web Proxy

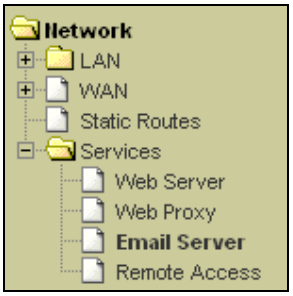


To configure the SMTP settings:

1. Click on **Services**.
2. Click on **Web Proxy**.

5.4 Email Server

You can configure how the InnGate will treat SMTP traffic from downstream clients.



To configure the SMTP settings:

1. Click on **Services**.
2. Click on **Email Server**.

Figure 5-2 shows the first part of the configuration interface:

1. **Display Email** – Any bounced or undelivered email will be forwarded to this email address.

Figure 5-2 Email Services Admin Contact

Figure 5-3 shows the SMTP settings configuration interface:

1. **Enable / Bypass / Disable SMTP Services –** Enable, bypass or disable SMTP services.

    a. **Enable –** By selecting this option all email will be sent using the defined SMTP server in the InnGate.

b. **Bypass –** This option allow users to use their own SMTP server. However, if the user's SMTP server is not resolvable, the defined SMTP server in the InnGate will be used.

c. **Disable –** Selecting this option will disable InnGate's SMTP setting and all email will be sent using the defined SMTP on user's mail setting.

2. **SMTP Host Name** – The InnGate can function as an SMTP server and this is the host name you must assign to it.

3. **Forward outgoing emails to another SMTP server** – If you need to use an external SMTP server (e.g. your ISP's SMTP) to send out emails, then the InnGate will need to be configured to forward all emails to it. If left unselected, the InnGate will use its own SMTP process for sending emails.

    a. **IP Address/Name** – IP address or host name of the SMTP server to forward outgoing emails to.

    b. **Port** – IP port of the SMTP service.

    ⚠ The SMTP server itself may have to be configured to allow relays from the InnGate (i.e. WAN IP address of the InnGate).

4. **Delete undeliverable emails after... hrs** – Duration before purging emails that could not be delivered.

5. **Set a domain name for outgoing emails without a domain name** – If selected, you can specify the domain name that the InnGate will append to the sender's email address if it finds the domain (e.g. alvin~~@antlabs.com~~) missing.

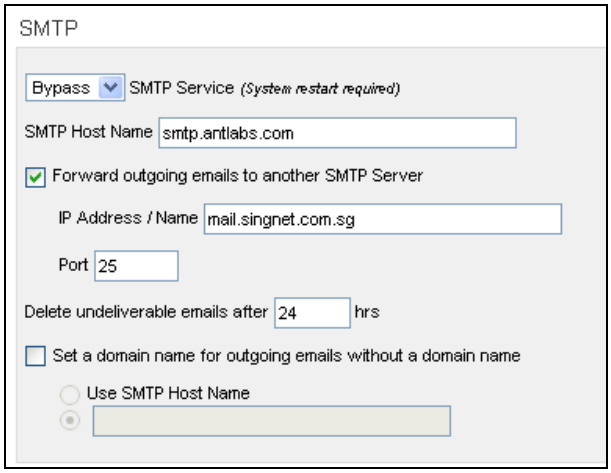


Figure 5-3 SMTP Settings

Figure 5-4 shows the interface for configuring the thresholds and checks performed on SMTP traffic.

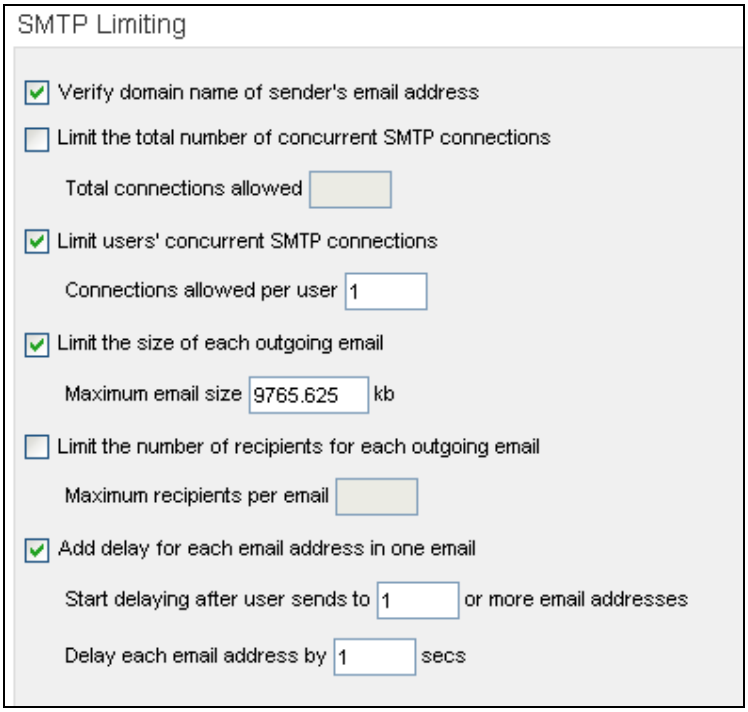

SMTP Limiting
Verify domain name of sender's email address
Limit the total number of concurrent SMTP connections
Total connections allowed
Limit users' concurrent SMTP connections
Connections allowed per user 1
Limit the size of each outgoing email
Maximum email size 9765.625 kb
Limit the number of recipients for each outgoing email
Maximum recipients per email
Add delay for each email address in one email
Start delaying after user sends to 1 or more email addresses
Delay each email address by 1 secs

Figure 5-4 SMTP Traffic Filters

The fields are described as follows:

1. **Verify domain name of sender's email address** – When enabled, the InnGate will ensure that the sender's email address contains a valid domain name before sending the email. Spam is often sent using fake email addresses.

2. **Limit the total number of concurrent SMTP connections** – This setting limits the total number of concurrent SMTP connections from all downstream clients. Software or viruses that spam usually send out high volumes of email concurrently, causing heavy bandwidth utilization and putting a strain on the resources of the InnGate.

3. **Limit the users' concurrent SMTP connections** – When enabled the InnGate will allow the specified number of concurrent SMTP connections per downstream client. This limits the effectiveness of malicious software which often attempt to send out high volumes of email through multiple concurrent SMTP connections.

4. **Limit the size of each outgoing email** – This setting limits the size of each email that can be sent out. Some malicious software attempt to overload the network resources such as by sending large emails, usually concurrently and to multiple recipients.

5. **Limit the number of recipients for each outgoing email** – When enabled, the InnGate will not send out emails that exceed the number of recipients specified here. Spam is often characterized by emails each addressed to a large number of recipients.

6. **Add delay for each email address in one email** – Spam is often sent in quick succession continuously to many recipients, resulting in high system loads. This setting reduces the effectiveness of automated spam systems by introducing artificial delays thus slowing down its ability to send.

The InnGate can also be configured to send an email to a user if he tries to access his POP3 server before having logged in to gain Internet access.

Figure 5-5 shows the interface for setting up such email reminders.

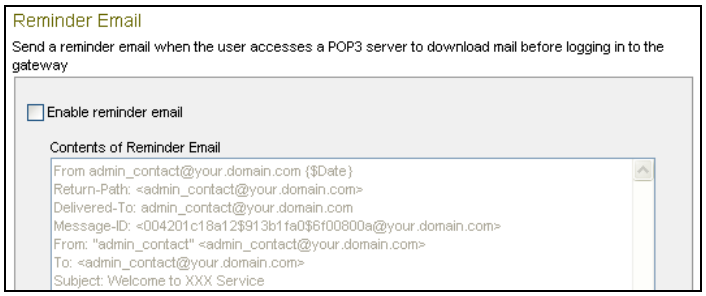


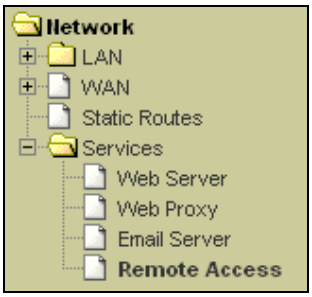
Figure 5-5 Reminder Email Template

Click Save to confirm the changes.

5.5 Remote Access

The InnGate provides FTP and Telnet services to allow the administrator to upload custom web pages and images or for remote administration.

⚠ Once the InnGate is fully configured, these services may not be necessary and can be disabled as a security measure.



To set the Remote Access settings:

1. Click on **Services**.
2. Click on **Remote Access**.

Select the appropriate services required as shown in Figure 5-6.

Click Save to confirm the changes.

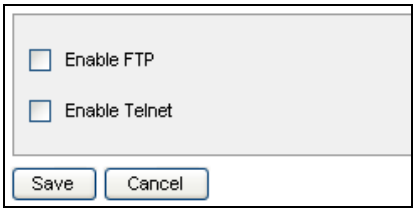


Figure 5-6 Remote Access Settings

5.5.1 Accessing the InnGate via Telnet and FTP

Telnet and FTP services are available on the InnGate and accessible from both the downstream and the upstream.

The default user ID and passwords are as follows:

Service	Unix Command to Connect to InnGate	Default User ID	Default Password
Telnet	telnet ezxcess.antlabs.com	console	admin
Ftp	ftp ezxcess.antlabs.com	ftponly	antlabs

The commands in the table above apply only to the clients connecting from the downstream. If you connect from the upstream, you should use the public host domain name or IP address assigned to it.

The Telnet and Console (see Section 8.12) services use the same user account and therefore share the same user ID and password to logon.

Chapter 6

SYSTEM MAINTENANCE AND DIAGNOSTICS

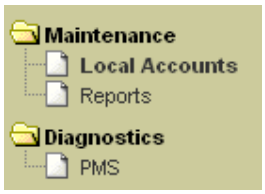
6.1 Overview

This chapter explains the system maintenance and diagnostics functions of the InnGate.

1. **Local Accounts Maintenance** – See Section 6.2.
2. **Reports Maintenance** – See Section 6.3.
3. **PMS Diagnostics** – See Section 6.4.

6.2 Local Accounts Maintenance

You can do maintenance of the local accounts you have been created by deleting expired accounts and email the list to an email address.



To do local accounts maintenance:

1. Click on **Local Accounts**.

Figure 6-1 shows the options for local accounts maintenance.

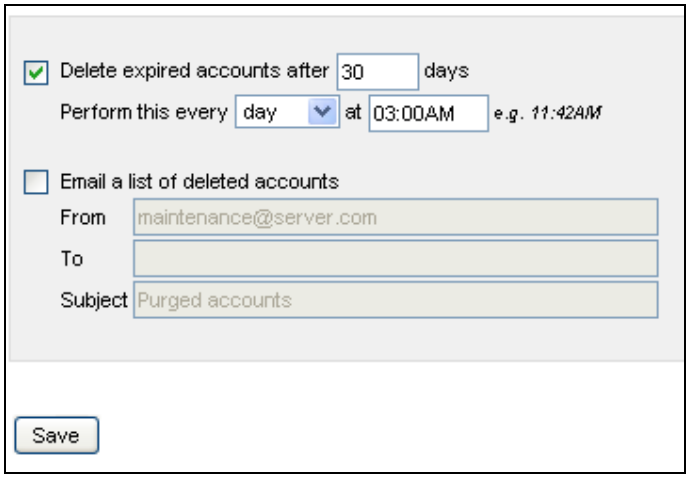


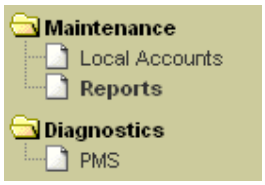
Figure 6-1 Local Accounts Maintenance

1. **Delete expired accounts after ... days –** This option enables deletion of accounts which have been expired for specified duration. The deletion can be scheduled daily, weekly, monthly.

2. **Email a list of deleted accounts –** To email the list of deleted accounts to an email address.

6.3 Reports Maintenance

You can schedule the system to auto-delete or email existing reports as part of routine maintenance.



To do reports maintenance:

1. Click on **Reports**.

Figure 6-2 shows the available reports to be selected for maintenance.

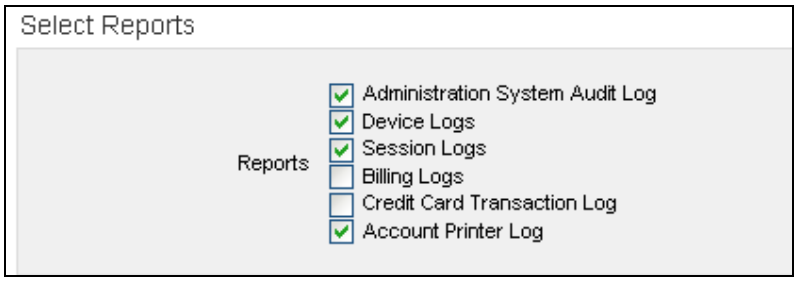


Figure 6-2 Select Reports

Figure 6-3 shows the task options that can be performed to the selected reports.

1. **Delete selected reports –** Selected reports will be deleted.

2. **E-mail selected reports as attachment –** A copy of the selected reports will be sent to the specified email address. If this option is selected, the fields must be completed:

    a. **From** – Specify the sender's email address.

    b. **To** – Specify the recipient's email address.

    c. **Subject** – Specify the Email subject.

3. **Compress attachment using ZIP** – The reports are compressed into a ZIP file before they are sent.

4. **Compress attachment using ZIP –** To compress the selected reports using ZIP to be attached in the email.

5. **Back-up selected reports to ... -** To back up the selected reports in /backup/reports FTP directory.

6. **Perform selected task(s) on record ... -** Specify how old records should be before they are deleted/emailed/backed up.

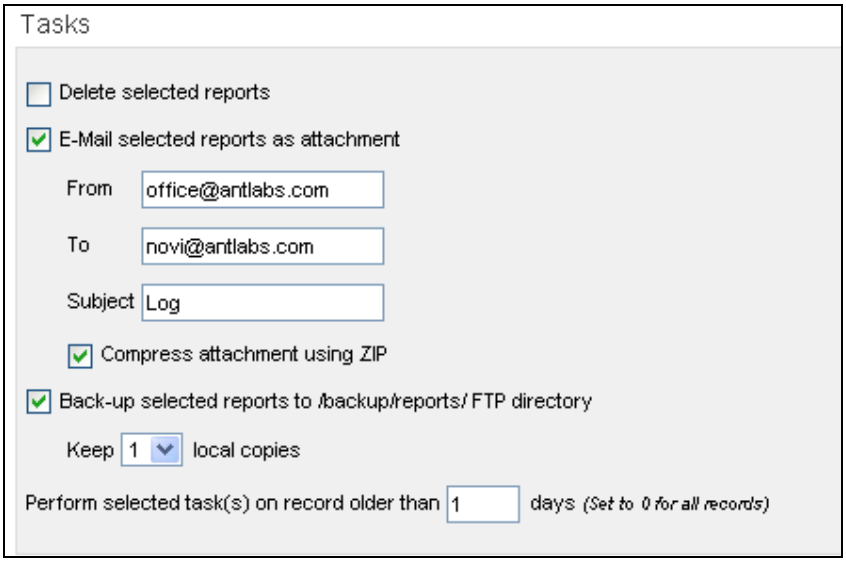


Figure 6-3 Maintenance Tasks

Figure 6-4 shows the interface for specifying the frequency of the tasks to be performed on the selected logs. The selected tasks can be scheduled daily, weekly or monthly.

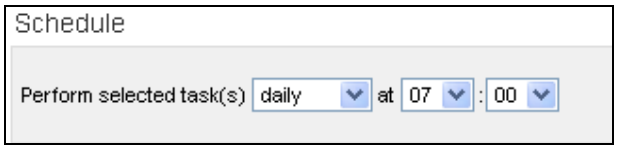


Figure 6-4 Maintenance Schedule

Click button

to view the advanced setting as shown in Figure 6-5.

1. **Do not format duration field into ... -** To change the duration format in the reports into readable format “hrs-mins-secs”.

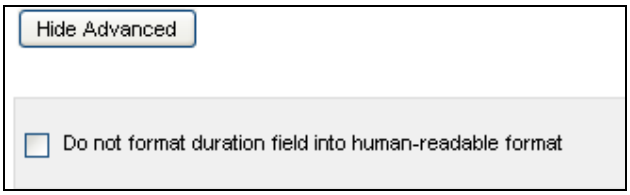


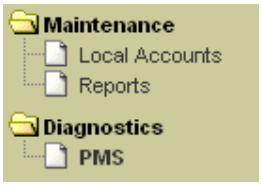
Figure 6-5 Maintenance Advanced Setting

Click Save to confirm the changes. Click Run Now to perform the maintenance immediately after the schedule is saved.

If both **Delete Selected Reports** and **E-mail Selected Reports** are selected, the reports are mailed to the recipient before they are deleted.

6.4 PMS Diagnostics

PMS Diagnostics allows you to do PMS test posting.



To do PMS diagnostics:

1. Click on **PMS**.

In order to do PMS test posting you need to fill the compulsory fields: room number, guest number, and amount into the form as shown in Figure 6-6. Click button Post.

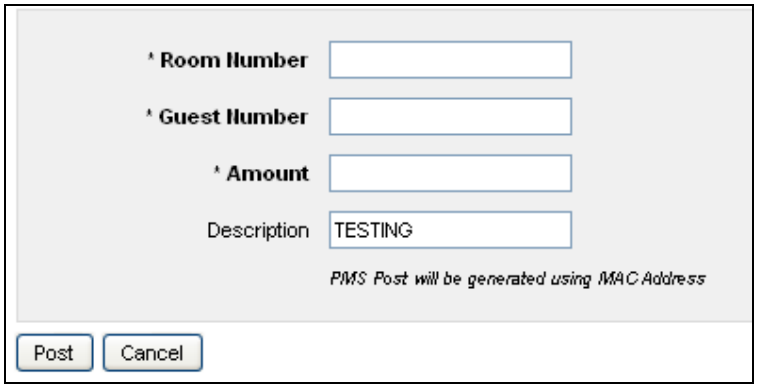
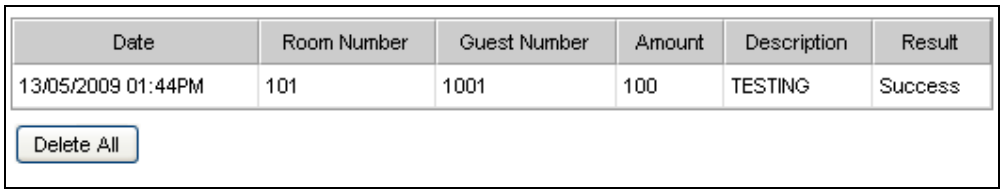


Figure 6-6 PMS Diagnostics

The information of posting you have done will be shown below the form as shown in Figure 6-7.



Date	Room Number	Guest Number	Amount	Description	Result
13/05/2009 01:44PM	101	1001	100	TESTING	Success

Delete All

Figure 6-7 Test Posting Log

Click button Delete All to clear the log.

Chapter 7

SYSTEM MONITORING AND REPORTING

7.1 Overview

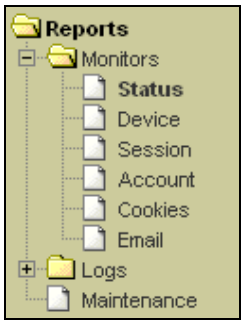
This chapter explains the system monitoring and reporting functions of the InnGate. These logs and reports can be used for troubleshooting and also for analysis purposes. You can also configure the presentation of the logs and reports:

1. **Monitors** – See Section 7.2.
2. **Logs** – See Section 7.3.
3. **Maintenance** – See Section 7.4.

7.2 Monitors

You can perform status, device, session, account, cookies and email monitoring.

7.2.1 Status Monitor



To monitor system status:

1. Click on **Monitors**.
2. Click on **Status**.

The System Status report includes information about:

1. **Downstream information** – Shows information about downstream devices.

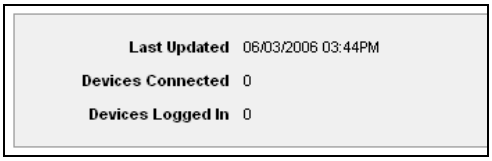


Figure 7-1 Downstream Devices

2. **Network information** – Shows LAN and WAN packet statistics.

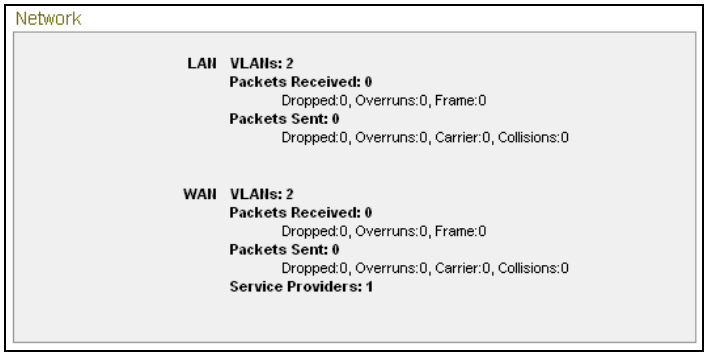


Figure 7-2 Network Information

3. **Appliance information** – Shows the system uptime, load, memory usage, etc.

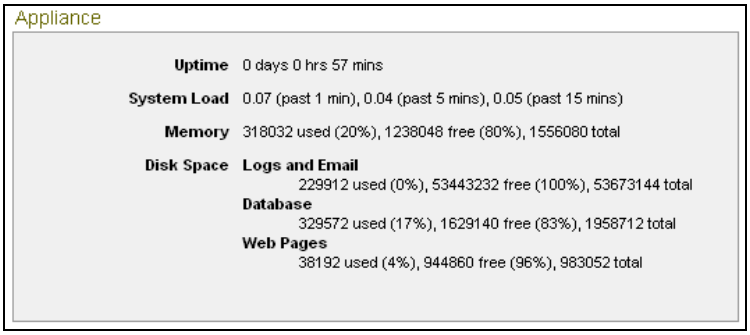

Appliance
Uptime 0 days 0 hrs 57 mins
System Load 0.07 (past 1 min), 0.04 (past 5 mins), 0.05 (past 15 mins)
Memory 318032 used (20%), 1238048 free (80%), 1556080 total
Disk Space Logs and Email
229912 used (0%), 53443232 free (100%), 53673144 total
Database
329572 used (17%), 1629140 free (83%), 1958712 total
Web Pages
38192 used (4%), 944860 free (96%), 983052 total

Figure 7-3 Appliance Information

Under normal operating conditions, the **Appliance** status should reflect the following:

1. **Users Connected** – This value should not exceed the user licenses for your InnGate.

2. **System Load** – This value should be less than 25 for the past 1, 5 or 15 minutes. Temporary high system loads may be observed when configuring or changing system settings. However, if observed for extended periods, you will need to check if the InnGate is experiencing an ARP storm, denial of service attacks, email spamming, etc.

3. **Disk Space** – The disk space used should be less than 80% for optimum performance. A common reason for high disk usage is the presence of large log files. It is recommended that you configure the InnGate's scheduled log maintenance settings (see Section 7.2) to regularly purge backdated log entries.

4. **Memory** – It is common for the memory used to be above 90% as the system maximizes the use of memory to cache commonly used data to improve system performance.

4. **Firmware information** – Shows the product, version, license information and serial numbers.

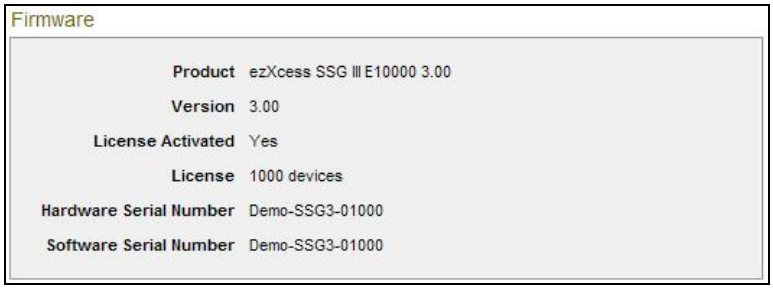
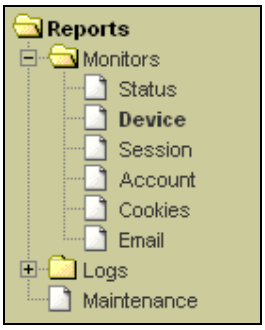


Figure 7-4 Firmware Information

Click button Refresh to refresh the InnGate's status summary.

7.2.2 Device Monitor

View real-time information about the devices detected on the downstream. Devices that have disconnected will be found in the **Device Logs**.



To view the Device Monitors:

1. Click on **Monitors**.
2. Click on **Device**.

Figure 7-5 shows the device monitor's interface when there are devices connected on the downstream.

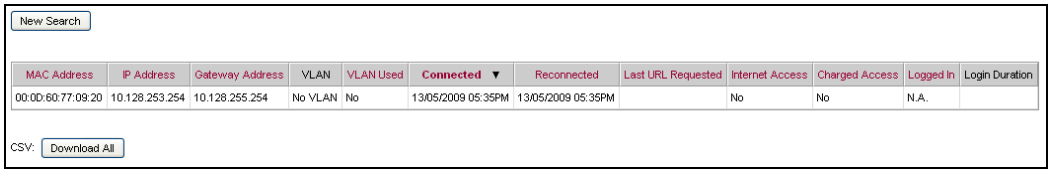


Figure 7-5 List of device detected

The following columns in the Device Monitors are further explained here:

1. **MAC Address**
2. **IP Address**
3. **Gateway Address**
4. **VLAN** – The name of the VLAN on which this device is detected.
5. **VLAN Used** – The VLAN ID.
6. **Connected** –
7. **Reconnected**
8. **Last URL Requested** –
9. **Internet Access** – This indicates whether the user can access the internet.
10. **Charged Access -** This indicates whether the user needs to login in order to get internet access.
11. **Logged In –** The start of login session (upon user login).
12. **Login Duration –** This indicates the duration of the login session.

Click "CSV: Download All" to export the entries into a comma-separated-values file.

Click New Search to run a search of the entries as shown in Figure 7-6.

You can click on the + button to add more search conditions or - to remove.

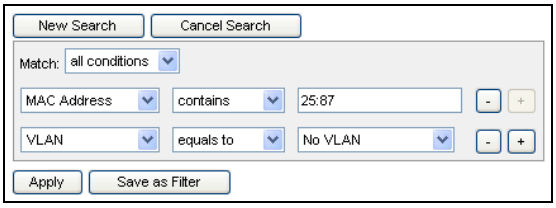


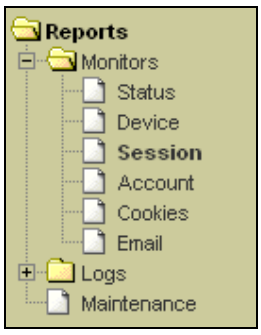
Figure 7-6 Search Device Log Entries

Click Apply to retrieve the entries with the search conditions applied.

Click Save as Filter to store the filter for future use.

7.2.3 Session Monitor

View real-time information about users currently logged in. Users who have logged out will be found in the **Session Logs**.



To view the Session Monitor:

1. Click on **Monitors**.
2. Click on **Session**.

Any active sessions will be listed as shown in Figure 7-7.

The following column in the Session Monitor is further explained here:

1. **Status** – Session status:
    a. **active** – The user has not logged out and the session is still active.
    b. **unexpired** – The user is physically disconnected from the network but the Usage Duration for the User has not been exceeded.
    c. **pending_close** – The user has logged out and the InnGate has initiated a Stop request to the RADIUS server and is awaiting a response from the RADIUS server.

Click "CSV: Download All" to export the entries into a comma-separated-values file.

Click Logout to logout any selected user sessions.

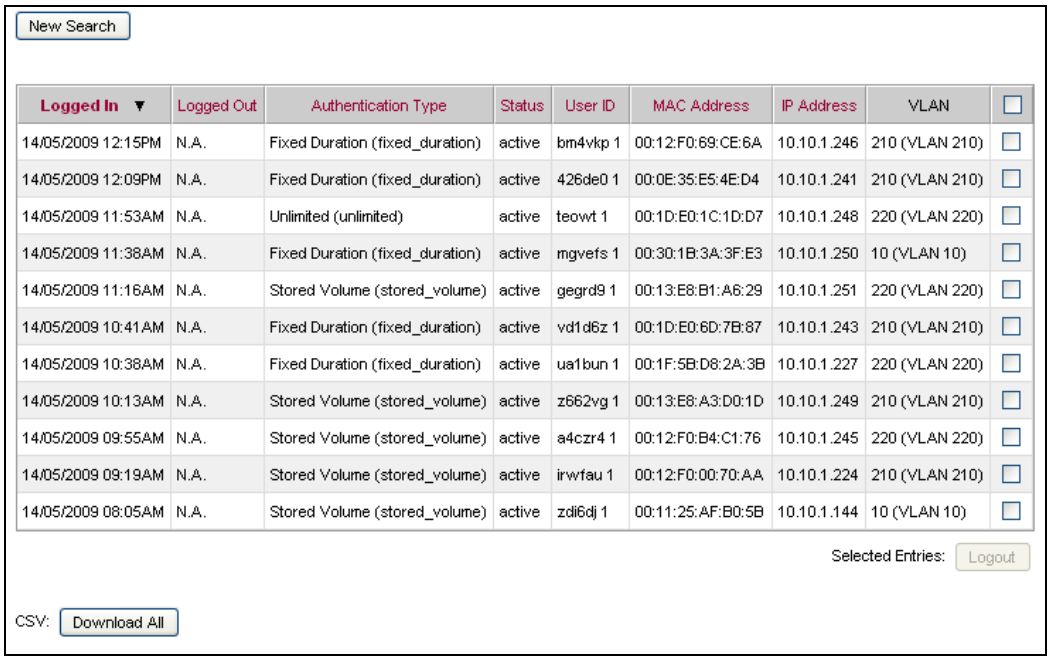

New Search
Logged In
Logged Out
Authentication Type
Status
User ID
MAC Address
IP Address
VLAN
14/05/2009 12:15PM N.A. Fixed Duration (fixed_duration) active bm4vkp 1 00:12:F0:69:CE:6A 10.10.1.246 210 (VLAN 210)
14/05/2009 12:09PM N.A. Fixed Duration (fixed_duration) active 426de0 1 00:0E:35:E5:4E:D4 10.10.1.241 210 (VLAN 210)
14/05/2009 11:53AM N.A. Unlimited (unlimited) active teowt 1 00:1D:E0:1C:1D:D7 10.10.1.248 220 (VLAN 220)
14/05/2009 11:38AM N.A. Fixed Duration (fixed_duration) active mgvefs 1 00:30:1B:3A:3F:E3 10.10.1.250 10 (VLAN 10)
14/05/2009 11:16AM N.A. Stored Volume (stored_volume) active gegrd9 1 00:13:E8:B1:A6:29 10.10.1.251 220 (VLAN 220)
14/05/2009 10:41AM N.A. Fixed Duration (fixed_duration) active vd1d6z 1 00:1D:E0:6D:7B:87 10.10.1.243 210 (VLAN 210)
14/05/2009 10:38AM N.A. Fixed Duration (fixed_duration) active ua1bun 1 00:1F:5B:D8:2A:3B 10.10.1.227 220 (VLAN 220)
14/05/2009 10:13AM N.A. Stored Volume (stored_volume) active z662vg 1 00:13:E8:A3:D0:1D 10.10.1.249 210 (VLAN 210)
14/05/2009 09:55AM N.A. Stored Volume (stored_volume) active a4czr4 1 00:12:F0:B4:C1:76 10.10.1.245 220 (VLAN 220)
14/05/2009 09:19AM N.A. Stored Volume (stored_volume) active irwfau 1 00:12:F0:00:70:AA 10.10.1.224 210 (VLAN 210)
14/05/2009 08:05AM N.A. Stored Volume (stored_volume) active zdi6dj 1 00:11:25:AF:B0:5B 10.10.1.144 10 (VLAN 10)
Selected Entries:
Logout
CSV:
Download All

Figure 7-7 List of Active Sessions

Click New Search to run a search of the entries as shown in Figure 7-8.

You can click on the + button to add more search conditions or - to remove.

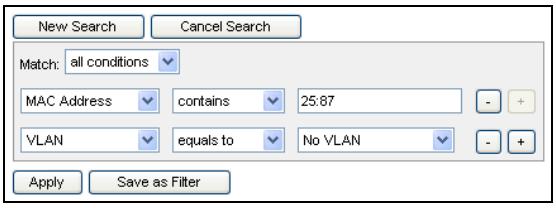


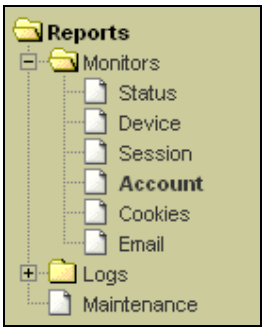
Figure 7-8 Search Session Entries

Click Apply to retrieve the entries with the search conditions applied.

Click Save as Filter to store the filter for future use.

7.2.4 Account Monitor

View all unexpired accounts' information that have been created.



To view the Account Monitor:

1. Click on **Monitors**.
2. Click on **Account**.

Any unexpired accounts will be listed as shown in Figure 7-9.

The following column in the Account Monitor is further explained here:

1. **User ID –** The user id of the user.
2. **Access Code –** The access code of the user.
3. **Plan –** The plan assigned the account.
4. **Valid Until –** This will show the expiry date of the account.
5. **Login Limit -** To show the login limit of the account.
6. **MAC Address –** To show the MAC address of the user when user is having session.
7. **Duration (Mins) –** To show the remaining duration user can use the account.
8. **Start Time –** The time when user starts using the account.
9. **End Time –** The time when user ends the session or to show the account's validity time.
10. **Remaining Volume (MB) –** To show the remaining volume of the account.

Search

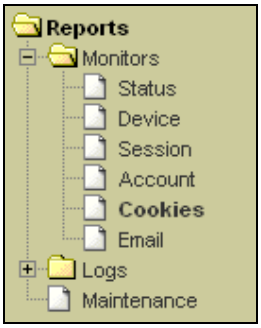
Enabled	User ID ▲	Access Code	Plan	Valid Until	Login Limit	MAC Address	Duration (mins)	Start Time	End Time	Remaining Volume (MB)
☑		fynry	Throttled		0 / -		Unlimited	01/01/1970 07:30AM		Throttled
☑	test		Throttled	13/05/2009 12:05:59	0 / -		Unlimited	01/01/1970 07:30AM		Throttled
☑		tester	tester		1 / -		Unlimited	13/05/2009 02:47AM		Unlimited
☑	wewwz		Throttled		0 / -		Unlimited	01/01/1970 07:30AM		Throttled
☑	zfjey		Throttled		0 / -		Unlimited	01/01/1970 07:30AM		Throttled

Figure 7-9 List of Accounts

⚠ The values shown in Accounts Monitor is not updated in real time. The MAC address is updated when user is using the account. The start time, end time, duration are updated only when user is not in the system.

7.2.5 Cookies Monitor

View cookies information of all valid sessions.



To view the Cookies Monitor:

1. Click on **Monitors**.
2. Click on **Cookies**.

Any valid session's cookies will be listed as shown in Figure 7-10.

The following column in the Cookies Monitor is further explained here:

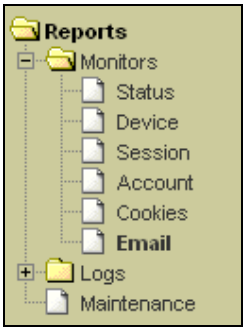
1. **Cookies ID –** The ID of cookies.
2. **User ID –** The user id whose cookies belong to.
3. **Last Used MAC Address –** The last used MAC address of relevant cookies.
4. **Cookie Expiry Date –** The validity time of session if it is set or 1 year after the cookies creation time if there is no session expiry time.

Cookie ID	User ID	Last Used MAC Address	Cookie Expiry Date
e5129fb01c82b3192a6763fb9b46f0a06573236c	a4czr4 1	00:12:F0:B4:C1:76	30/05/2009 11:00PM
a3899f539b074991e400bf3d4a359ecbb57c1e02	crhdnu 1	00:12:F0:12:9D:69	30/05/2009 11:00PM
34e8cd70e54cec9007559af866476d04f0b0c187	gegrd9 1	00:13:E8:B1:A6:29	30/05/2009 11:00PM
edc9e6cd72310461f5896374daf9fb95b3fe3fae	teowt 1	00:1D:E0:1C:1D:D7	14/05/2010 07:18PM
58d1ea0853d4e5a894df4116f8c2f185c69efb39	xyxixq 1	00:16:E6:D9:FD:99	30/05/2009 11:00PM
73d981e0bed7b07a6d033452ec9af5f0c07cd0f2	zdi6dj 1	00:11:25:AF:B0:5B	30/05/2009 11:00PM
28e282bfb511831d45df6182e8246bbd88b46450	mgvefs 1	00:30:1B:3A:3F:E3	14/05/2009 03:38PM
73776524c66e398460e7a3e601b4a984143f94f6	jhmwry 1	00:1F:5B:D8:2A:3B	30/05/2009 11:00PM
ff748abfd7a61e4ff7a05442901a45df3be4a66d	7rbfmk 1	00:13:E8:B6:0E:53	30/05/2009 11:00PM
9966cf5ad9a60b87757e1a744c129b7cc307b0f0	a16b4g 1	00:12:F0:69:CE:6A	14/05/2009 03:58PM
6552e2b1ab20e574b22854f3a0990d48a650622b	irwfau 1	00:12:F0:00:70:AA	30/05/2009 11:00PM
a7cef4d1e1762c300858b4a5935a7fa8d0ac2fed	ua1bun 1	00:1F:5B:D8:2A:3B	14/05/2009 02:38PM
19aed916bbbe63b8f43c4378fe42a6d35c58afa3	gegrd9 1	00:13:E8:B1:A6:29	30/05/2009 11:00PM
642ad643172e452f39f2c5a8abe9e5d1d58b597f	z662vg 1	00:13:E8:A3:D0:1D	30/05/2009 11:00PM
1128ac2c18c2b7a4adbf6336b6e185ed02acf299	724174 1	00:22:41:C4:6D:03	14/05/2009 02:55PM
890658c1406dea41a5a66fabf6c92b9e96069649	bwkpn 1	00:19:21:90:28:23	29/05/2009 11:00PM
8ae38d0f23b7b8bbf5be7b98156fc02435a4a60f	426de0 1	00:0E:35:E5:4E:D4	21/05/2009 12:09PM
870176243e3ff399cb4ab4e147b5644103f719c5	vd1d6z 1	00:1D:E0:6D:7B:87	14/05/2009 02:41PM

Figure 7-10 List of Cookies

7.2.6 Email Monitor

This function shows the number of undelivered emails as well as the amount of disk space used to store emails that have yet to be sent out.



To view the Email Monitor:

1. Click on **Monitors**.
2. Click on **Email**.

The email monitor status shows number of undeliverable emails and size of disk space used.

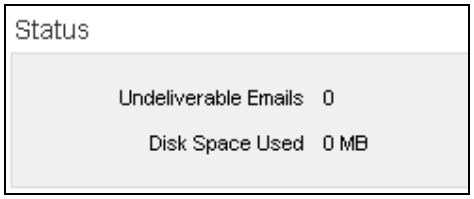


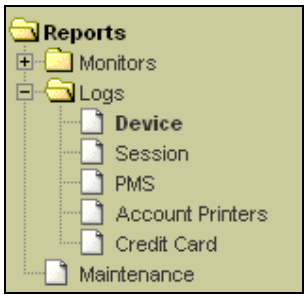
Figure 7-11 Email Monitor Status

7.3 Logs

Logs shows past activity of downstream devices, sessions, PMS (when available), account printer and credit card (when available).

7.3.1 Device Logs

View past activity of downstream devices that are now disconnected. Devices that are still detected on the downstream will be found in **Device Monitor**.



To view the Device Logs:

1. Click on **Logs**.
2. Click on **Device**.

Any existing log entries will be listed as shown in Figure 7-12.

Click "CSV: Download All" to export the existing log entries into a comma-separated-values file.

Click Delete All Entries to purge the log.

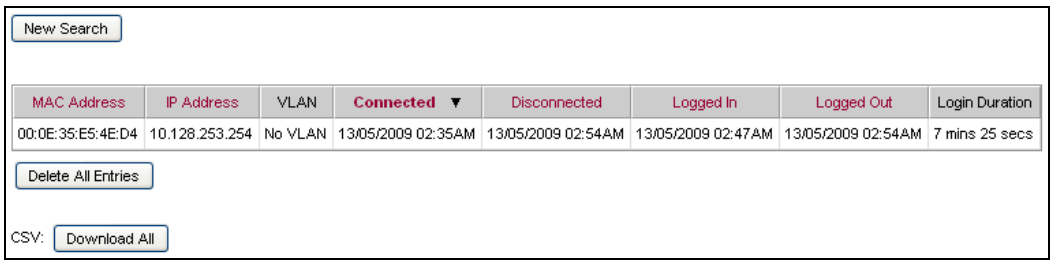


Figure 7-12 Device Logs

Click New Search to run a search of the log entries as shown in Figure 7-13.

You can click on the + button to add more search conditions or - to remove.

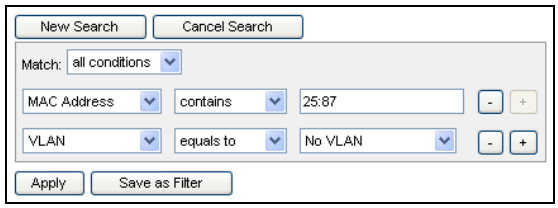


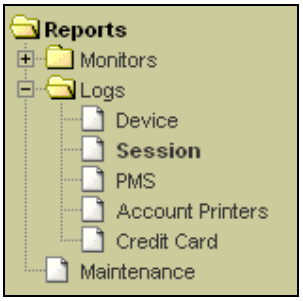
Figure 7-13 Search Device Log Entries

Click Apply to retrieve the log entries with the search conditions applied.

Click Save as Filter to store the filter for future use.

7.3.2 Session Logs

View the log of past user sessions. Currently active sessions are displayed in **Session Monitor** instead.



To view the Device Logs:

1. Click on **Logs**.
2. Click on **Session**.

Any existing log entries will be listed as shown in Figure 7-14.

Click "CSV: Download All" to export the existing log entries into a comma-separated-values file.

Click Delete All Entries to purge the log.

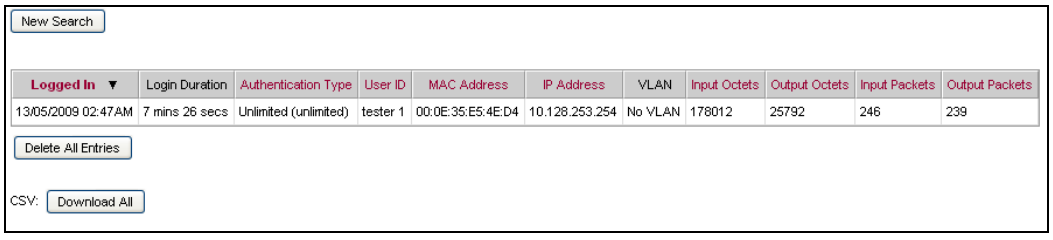


Figure 7-14 Session Logs

Click New Search to run a search of the log entries as shown in Figure 7-15.

You can click on the + button to add more search conditions or - to remove.

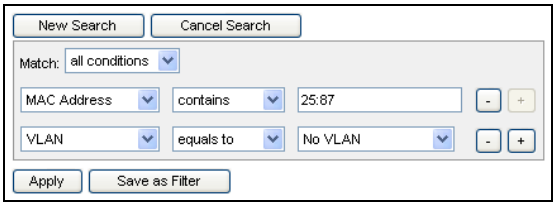


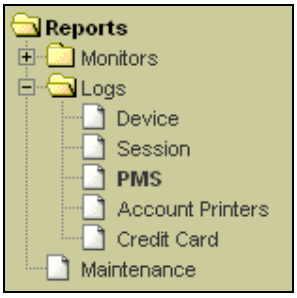
Figure 7-15 Search Session Log Entries

Click Apply to retrieve the log entries with the search conditions applied.

Click Save as Filter to store the filter for future use.

7.3.3 PMS Logs

View the log of PMS billing, room status, and guest status.



To view the PMS Logs:

3. Click on **Logs**.
4. Click on **PMS**.

Click on Billing Log tab to view the past PMS billing log as shown in Figure 7-13.

The following column in the PMS Billing Log is further explained here:

1. **Date –** Date of billing
2. **Guest Number**
3. **Room Number –** Current room number.
4. **Original Room Number –** Previous room number (if guest ever changed room).
5. **Usage Time**
6. **Start Time**
7. **Charge Start Time**
8. **Amount –** Amount of the billing.

9. **Status**

10. **MAC Address**

11. **Description –** Description of the billing.

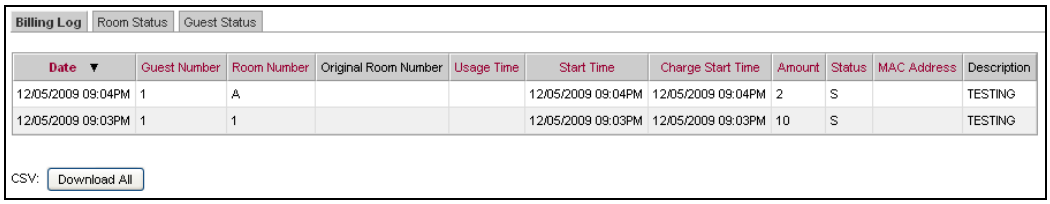


Figure 7-13 PMS Billing Log

Click "CSV: Download All" to export the existing log entries into a comma-separated-values file.

Click on Room Status tab to view the log of room status as shown in Figure 7-16.

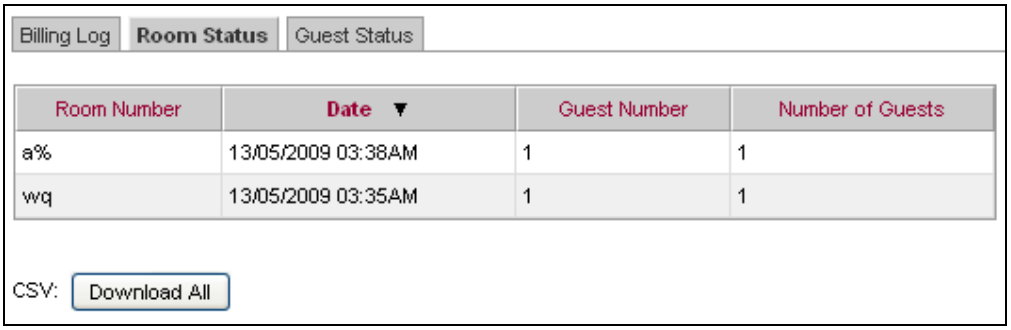


Figure 7-16 PMS Room Status Log

Click "CSV: Download All" to export the existing log entries into a comma-separated-values file.

Click on Guest Status tab to view the log of guest status as shown in Figure 7-17.

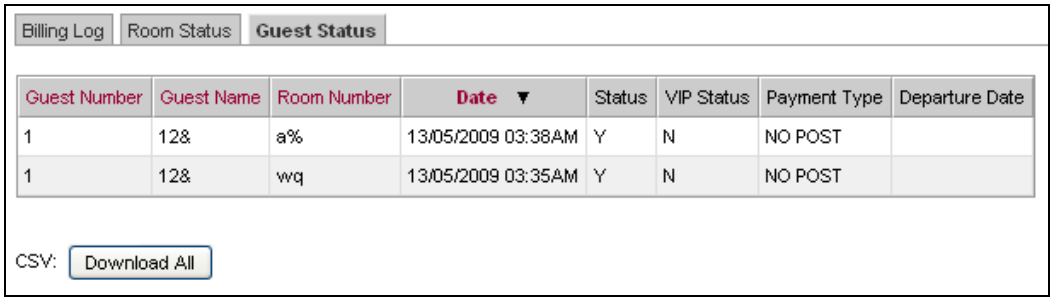
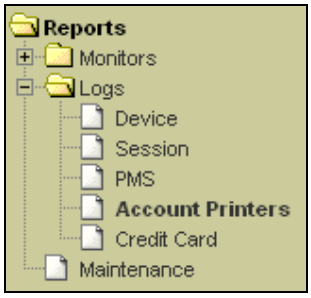


Figure 7-17 PMS Guest Status Log

7.3.4 Account Printer Logs

View the log of accounts created by account printers.



To view the Account Printer Logs:

1. Click on **Logs**.
2. Click on **Account Printers**.

Figure 7-18 shows the list of accounts created by account printers.

The following column in the Account Printers Log is further explained here:

1. **Date & Time** – The date and time when the relevant account is created.
2. **Printer IP address** – The IP address of the printer.
3. **Button** – To indicates which button was pressed to create the account.
4. **User ID**
5. **Password**
6. **Access Code**

Date & Time	Printer IP Address	Button	User ID	Password	Access Code	☐
2009-05-13 22:34:52	10.40.1.202	Press A			fynry	☑
2009-05-13 22:45:18	10.40.1.202	Press A			yinsi	☐
2009-05-13 22:48:25	10.40.1.202	Press A			unn7i	☐
2009-05-13 22:48:47	10.40.1.202	Press B	jjsiz	t4f9h		☐

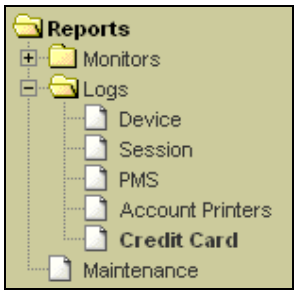
Delete All | Download All CSV | Selected Entries: Delete | Download CSV

Figure 7-18 Account Printers Log

Click button Delete to delete selected entries or click button Delete All to delete all the logs. Click button Download CSV to download selected entries in comma-separated-values format or click button Download All CSV to download all the logs in comma-separated values format.

7.3.5 Credit Card Logs

View the log of past credit card activities.



To view the Credit Card Logs:

3. Click on **Logs**.
4. Click on **Account Printers**.

Figure 7-19 shows the log of credit card.

Date ▼	Local Transaction ID	Payment Gateway Transaction ID	MAC Address	IP Address	VLAN	Plan	Price	Payment Gateway	Transaction Status	Transaction Details
14/05/2009 12:09PM	46	V78A1BDB4E28	00:0E:35:E5:4E:D4	10.10.1.241	210 (VLAN 210)	Fixed Duration 6 hours	10.00	Paypal Payflow Link	Transaction Completed	
14/05/2009 12:02PM	45	V18A1D22376F	00:0C:F1:07:2E:35	10.10.1.252	210 (VLAN 210)	Fixed Duration 6 hours	10.00	Paypal Payflow Link	Transaction Completed	
14/05/2009 12:02PM	44		00:0C:F1:07:2E:35	10.10.1.252	210 (VLAN 210)	Fixed Duration 6 hours	10.00	Paypal Payflow Link	Transaction Started	
14/05/2009 12:01PM	43	0	00:0C:F1:07:2E:35	10.10.1.252	210 (VLAN 210)	Fixed Duration 6 hours	10.00	Authorize.Net SIM	Transaction Completed	
14/05/2009 11:59AM	42	V79A1BDB47A0	00:0C:F1:07:2E:35	10.10.1.252	210 (VLAN 210)	Fixed Duration 6 hours	10.00	Paypal Payflow Pro	Transaction Completed	

Figure 7-19 Credit Card Log

7.4 Maintenance

Reports maintenance has been explained in Section 6.3.

Chapter 8

SYSTEM ADMINISTRATION

8.1 Overview

This chapter covers some of the common system configuration options and maintenance tasks:

1. **Setting up Administrator Accounts** – See Section 8.2.
2. **Powering up and shutting down the system** – See Section 8.3.
3. **System Configuration Backup or Restore** – See Section 8.4.
4. **Applying System Patches** – See Section 8.5.
5. **Setting the Date and Time** – See Section 8.6.
6. **Syslog Configuration** – See Section 8.7.
7. **SNMP Setup** – See Section 8.8.
8. **View API Information** – See Section 8.9.
9. **High Availability** – See Section 8.10.
10. **View License Information** – See Section 8.11.
11. **Console Access via Serial Connection** – See Section 8.12.
12. **Securing the System for Deployment** – See Section 8.13.

8.2 Setting up Administrator Accounts

Administrator accounts with different access privileges can be created for personnel with different responsibilities.
Few processes in setting up admin accounts are:

1. **Creating an Administrator Group** – See Section 8.2.1.
2. **Defining Admin Group Permissions** – See Section 8.2.2.
3. **Creating an Administrator Account** – See Section 8.2.3.

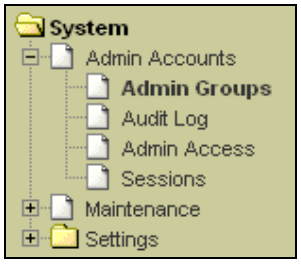
4. **Viewing Audit Log** – See Section 8.2.4.

5. **Assigning Admin Access** – See Section 8.2.5.

6. **Viewing Sessions** - See Section 8.2.6.

8.2.1 Creating an Administrator Group

In this step, you will define the administrator groups for different sets of administrator accounts.



To create an administrator group:

1. Click on **Admin Accounts**.
2. Click on **Admin Groups**.

Select the **Groups** tab as shown in Figure 8-1.

Any existing entries will be displayed. Click on an entry to modify it or click Add to create one.

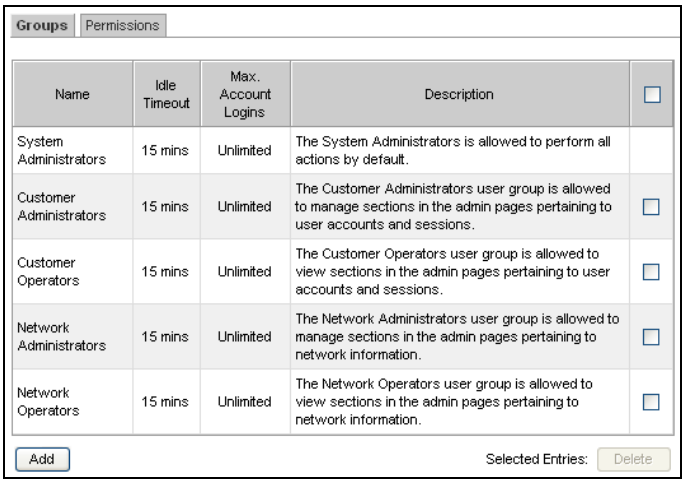

Groups
Permissions
Name
Idle Timeout
Max. Account Logins
Description
System Administrators
15 mins
Unlimited
The System Administrators is allowed to perform all actions by default.
Customer Administrators
15 mins
Unlimited
The Customer Administrators user group is allowed to manage sections in the admin pages pertaining to user accounts and sessions.
Customer Operators
15 mins
Unlimited
The Customer Operators user group is allowed to view sections in the admin pages pertaining to user accounts and sessions.
Network Administrators
15 mins
Unlimited
The Network Administrators user group is allowed to manage sections in the admin pages pertaining to network information.
Network Operators
15 mins
Unlimited
The Network Operators user group is allowed to view sections in the admin pages pertaining to network information.
Add
Selected Entries:
Delete

Figure 8-1 List of Admin Groups

Figure 8-2 shows the interface for configuring the Admin Group:

1. **Name** – The name given to the Admin Group.

2. **Idle Timeout** – Maximum inactivity period before auto log off.

3. **Max. Account Logins** – Maximum number of accounts in the group that can concurrently login.

4. **Description** – A description for this entry.

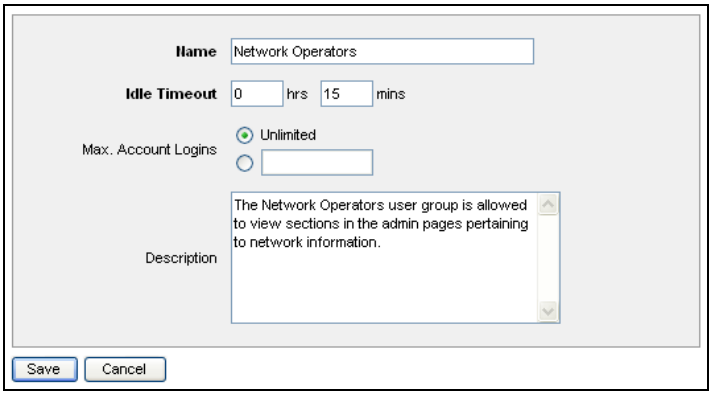
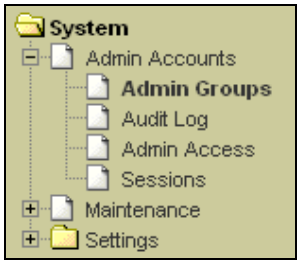


Figure 8-2 Admin Group Configuration

Click Add to confirm the entry (or Save for modifications).

8.2.2 Defining Admin Group Permissions

In this step, you will define the permissions for the Admin Group created.



To define administrator group permissions:

1. Click on **Admin Accounts**.
2. Click on **Admin Groups**.

Select the **Permissions** tab as shown in Figure 8-3.

All Admin Groups will be listed and you can click View Permissions > to view the permissions for each.

Click on the Admin Group's name to modify the permissions for it.

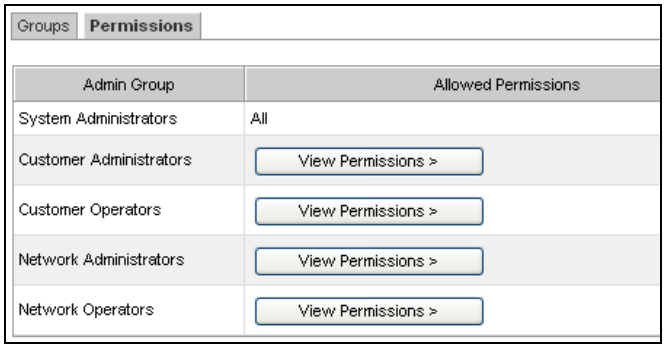


Figure 8-3 List of Admin Groups and Permissions

Figure 8-4 shows the list of permissions that can be configured for the selected Admin Group.

Select the checkboxes for the permissions you wish to give to the group.

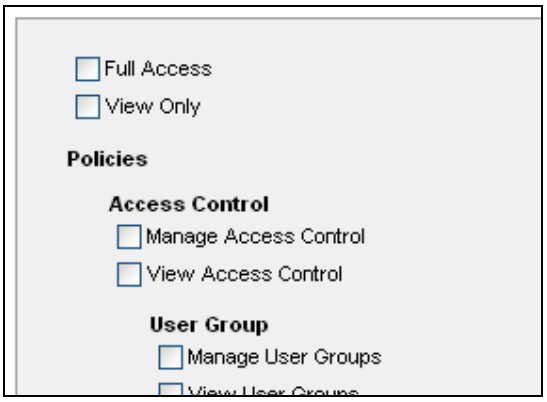
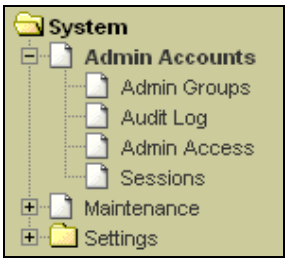


Figure 8-4 Admin Group Permissions

Click Save to confirm the changes.

8.2.3 Creating an Administrator Account

In this step, you will create Admin Accounts that will be given out to the respective personnel.



To create an administrator account:

1. Click on **Admin Accounts**.

Any existing entries will be displayed (see Figure 8-5). Click on an entry to modify it or click Add to create one.

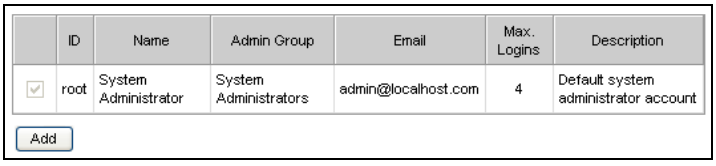


Figure 8-5 List of Administrator Accounts

Figure 8-6 shows the interface for configuring the Admin Account:

1. **Enabled** – Select to activate the account.
2. **ID** – Login user ID.
3. **Name** – The name given to the account.
4. **Password / Re-type Password** – Login password.
5. **Admin Group** – Select the admin group.
6. **Email** – The email address for the user account.
7. **Max. Logins** – Maximum number of concurrent sessions allowed for this account. Earlier sessions will be terminated when the limit is exceeded.
8. **Description** – A description for this entry.

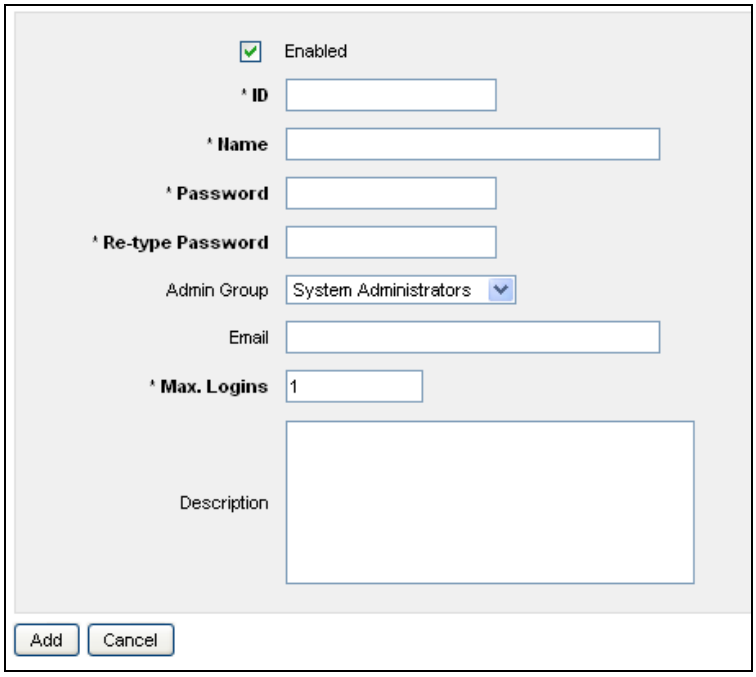
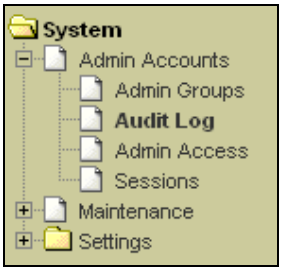


Figure 8-6 Administrator Account Details

Click Add to confirm the entry (or Save for modifications).

8.2.4 Viewing Audit Log



To access the option:

1. Click on **Admin Accounts**.
2. Click on **Audit Log**.

Figure 8-7 shows the existing list of audit log:

1. **Date & Time –** The date and time when the admin account logged in.
2. **ID –** The admin account used for login.
3. **Status –** The status of login.
4. **Module –** The module accessed by admin.
5. **Operation –** The activity done by admin.
6. **Details –** Additional information of activity.

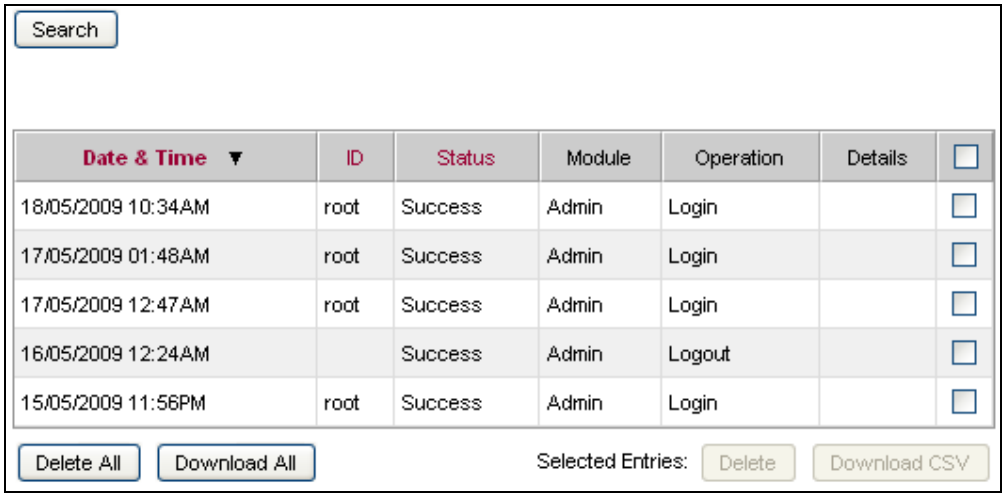
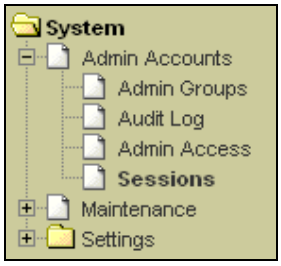


Figure 8-7 Audit Log

8.2.5 Assigning Admin Access

Assigning Admin Access is explained in Section 8.13.1.

8.2.6 Viewing Sessions



To access the option:

1. Click on **Admin Accounts**.
2. Click on **Sessions**.

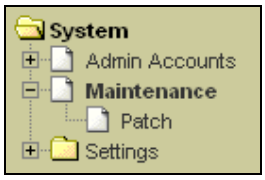
Figure 8-8 shows the existing admin account sessions:

1. **ID**
2. **Name**
3. **Admin Group**
4. **Login Time**
5. **Current Session**

ID	Name	Admin Group	Login Time	Current Session
root	System Administrator	System Administrators	18/05/2009 09:44AM	☑

Figure 8-8 Admin Account Sessions

8.3 Powering up and shutting down the system



To access the power options:

1. Click on **Maintenance**.

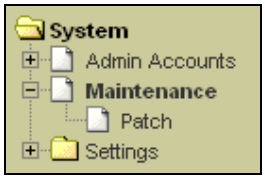
Figure 8-9 shows the power options interface.

Click Restart to reboot the InnGate.

Click Shut Down to power down the InnGate.

Figure 8-9 Power Options

8.4 System Configuration Backup or Restore



To access the Backup/Restore options:

1. Click on **Maintenance**.

Figure 8-10 shows the interface for performing a backup or restore of the system configuration:

1. **System Configuration Backup** – Choose "Download" optionto save a copy of the system's configuration into a binary-format file. Or you can also choose "Save to local system" to save the configuration file in the local drive. Click button Backup to back up. This process normally takes less than a minute as the InnGate gathers the system configuration into a binary file.

   The file will be named "configuration_yyyymmdd.ezxconf", where yyyymmdd is the current date in year-month-date format (E.g. 2 Jun 2006 = 20060602).

2. **System Configuration Restore** – Click Browse... to select the system configuration backup binary file to use and then click Restore.

   ⚠ Reboot the InnGate after performing a system restore.

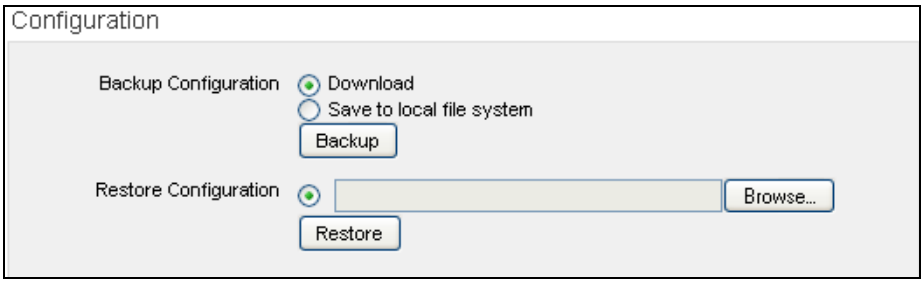


Figure 8-10 Backup and Restore functions

After you have made a backup of the system configuration, you should also make a backup of the directories containing any customized web pages such as login scripts:

1. Access the InnGate via FTP (see Section 5.5.1).

2. Browse the directories using "`ls -l`" and identify those files/directories you wish to make a backup of.

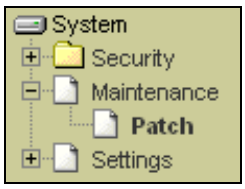
3. Change to the temporary directory on the local host using the "`lcd`" command so that whatever you download will end up in that directory. E.g. "`lcd c:\backup`".

4. Copy out the files/directories you wish to make a backup copy of using the "`mget`" command. E.g. "`mget sample`".

In addition to backing up and restoring the configuration of a InnGate, the Command Line Interface (CLI) provides additional features to make a snapshot of the current state of the gateway and perform a subsequent on-demand restore. You can also invoke a factory restore from the CLI to revert the InnGate back to its original state. Please refer to the InnGate **Command Line Interface Reference** for further information.

8.5 Applying System Patches

System patches are released occasionally to fix bugs and correct problems or in response to security vulnerabilities as part of ANT*labs*' continuous product support commitment.



To apply a system patch:

1. Click on **Maintenance**.

2. Click on **Patch**.

Figure 8-11 shows the interface for applying a patch. Any existing patches are listed in the **Installed Patches** table.

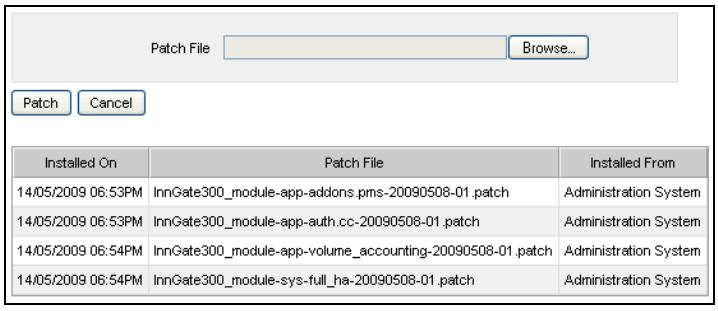


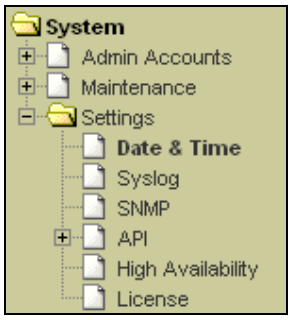
Figure 8-11 Patch Application Interface

Click Browse... to select the patch file.

Then click Patch to apply the selected patch file.

⚠ Patches must be applied in the exact sequence of release, earlier patches first followed by later patches. And no patch should be skipped. Failure to comply may result in system corruption.

8.6 Setting the Date and Time



To set the Date and Time:

1. Click on **Settings**.
2.
3. Click on **Date & Time**.

Figure 8-12 shows the Date and Time configuration page:

1. **Retrieve time from NTP server** – The InnGate supports Network Time Protocol (NTP) to automatically synchronize the internal clock with an external time server.

    a. **IP Address** – NTP server IP address.

2. **New Date & Time** – Specify the updated date and time here.

3. **Time Zone** – Specify the time zone that the InnGate is in. You will need to restart the InnGate.

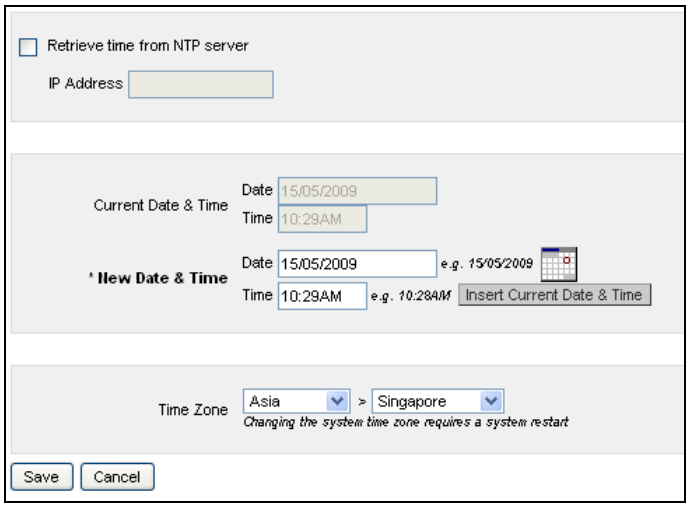
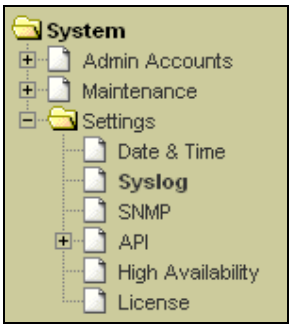


Figure 8-12 Date and Time Settings

Click Save to confirm the changes.

8.7 Syslog Configuration

System logs can be sent to a remote Syslog server. Syslog is a standard protocol for sending log information over TCP/IP, usually using UDP Port 514.



To configure Syslog:

1. Click on **Settings**.
2. Click on **Syslog**.

Figure 8-13 shows the Syslog selection settings:

1. **Mirror system logs...** – When selected the following system log information is sent to the Syslog server:
    a. **Email information**
    b. **FTP login/logout information**
2. **IP Address** – The IP address of the Syslog server to send to.

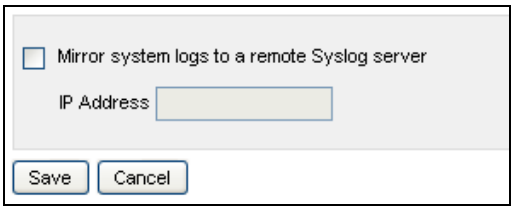


Figure 8-13 Syslog Settings

Click Save to confirm the changes.

Figure 8-14 shows the sample output on a typical Syslog daemon/server.

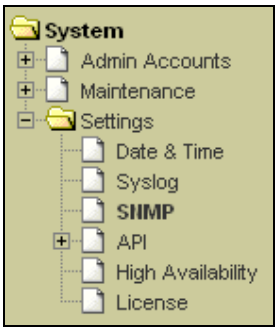
Date	Time	Priority	Hostname	Message
07-07-2005	17:06:11	System1.Info	127.128.50.254	ftpd[17049]: FTP session closed
07-07-2005	17:06:08	System1.Info	127.128.50.254	ftpd[17049]: FTP LOGIN FROM 192.168.122.116 [192.168.122.116], ftponly
07-07-2005	17:02:07	Mail.Info	127.128.50.254	qmail: 1120723988.610783 end msg 337
07-07-2005	17:02:07	Mail.Info	127.128.50.254	qmail: 1120723988.610754 status: local 0/10 remote 0/20
07-07-2005	17:02:07	Mail.Info	127.128.50.254	qmail: 1120723988.610649 delivery 8928: success: 165.21.103.137_accepted_message./Remote_host_said:_250_2.0.0_j679273b002103_Message_accepted_for_deliv
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.863200 status: local 0/10 remote 1/20
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.863085 delivery 8929: success: 165.21.103.137_accepted_message./Remote_host_said:_250_2.0.0_j67924vS001227_Message_accepted_for_deliv
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.555482 status: local 0/10 remote 2/20
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.555376 delivery 8927: success: 165.21.103.137_accepted_message./Remote_host_said:_250_2.0.0_j67924ua001226_Message_accepted_for_deliv
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.438288 status: local 0/10 remote 3/20
07-07-2005	17:02:04	Mail.Info	127.128.50.254	qmail: 1120723985.438182 delivery 8926: success: 165.21.103.137_accepted_message./Remote_host_said:_250_2.0.0_j67924fL001225_Message_accepted_for_deliv
07-07-2005	17:01:59	Mail.Info	127.128.50.254	smtpd: 1120723980.897470 tcpserver: status: 0/200
07-07-2005	17:01:59	Mail.Info	127.128.50.254	smtpd: 1120723980.896755 tcpserver: end 26197 status 0
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.819481 status: local 0/10 remote 4/20
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.819367 delivery 8925: success: 165.21.6.30_accepted_message./Remote_host_said:_250_2.0.0_j6791xdu008154_Message_accepted_for_delivery/
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.554695 status: local 0/10 remote 5/20
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.554591 starting delivery 8929: msg 337 to remote teowt@antlabs.com
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.543355 status: local 0/10 remote 4/20
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.543268 starting delivery 8928: msg 337 to remote aw@antlabs.com
07-07-2005	17:01:59	Mail.Info	127.128.50.254	qmail: 1120723980.542467 status: local 0/10 remote 3/20

Figure 8-14 Syslog Server Output

⚠ Some Syslog servers may require you to specify the sender's IP address as a security measure. In such cases, you should specify the WAN IP address of the InnGate.

8.8 SNMP Setup

The InnGate supports **SNMP version 2** and can be configured to operate in an SNMP enabled managed network environment as a network element. Network managers can then query the Management Information Base (MIB) maintained by the InnGate for remote monitoring.



To configure SNMP:

1. Click on **Settings**.
2. Click on **SNMP**.

Figure shows the interface for setting the Community string for authentication purposes.

Figure 8-15 SNMP Community String

Figure 8-16 shows the interface for configuring SNMP traps:

1. **Destination Host** – Host IP address of the manager that traps will be sent to. By default it is set to 127.0.0.1 which means that traps will not be sent out.
2. **Port** – SNMP traps are normally sent on port 162.
3. **Community** – The community string of the manager for authentication when sending traps to it.

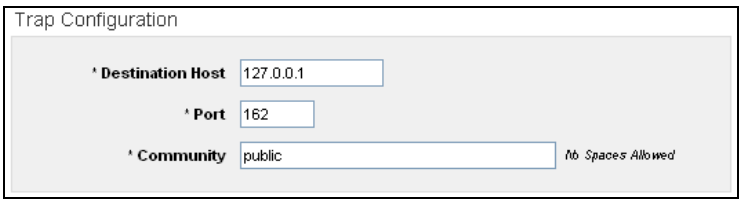


Figure 8-16 Trap Configuration

Figure 8-17 shows the SNMP Denial of Service trap suppressor configuration.

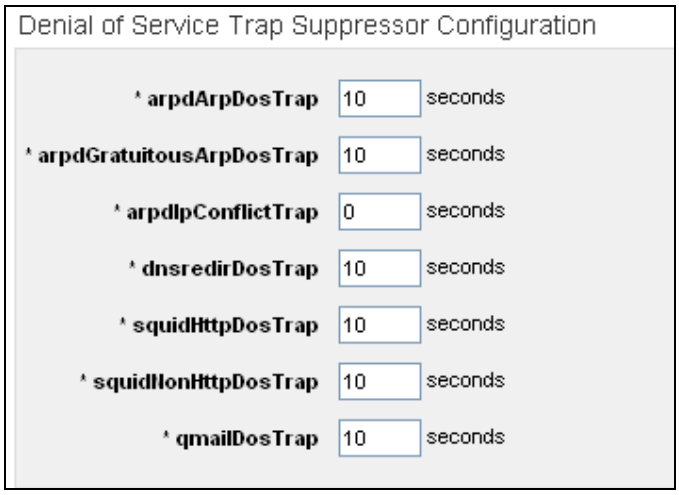

Denial of Service Trap Suppressor Configuration
* arpdArpDosTrap 10 seconds
* arpdGratuitousArpDosTrap 10 seconds
* arpdIpConflictTrap 0 seconds
* dnsredirDosTrap 10 seconds
* squidHttpDosTrap 10 seconds
* squidNonHttpDosTrap 10 seconds
* qmailDosTrap 10 seconds

Figure 8-17 Denial of Service Trap Suppressor Configuration

Figure 8-18 shows the SNMP system information configuration.

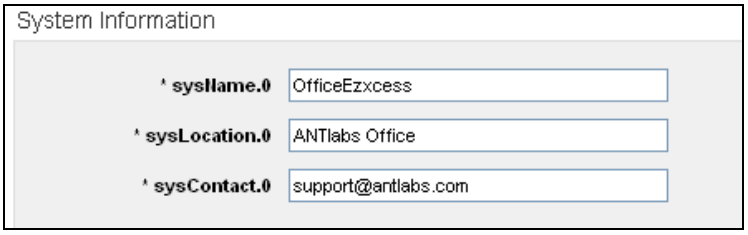


Figure 8-18 System Information

Click Save to confirm the changes.

8.8.1 Traps Generated

The following are the process information SNMP traps sent by the InnGate:

Process/Trap Ref	Description	OID
ARPD	ARPD service down	.1.3.6.1.4.1.12902.1.1.3.2.1.0
MYSQLD	Database service down	.1.3.6.1.4.1.12902.1.1.3.2.2.0
ARPD_MONITOR	ARPD_mon service down	.1.3.6.1.4.1.12902.1.1.3.2.3.0
SQUID	Web proxy service down	.1.3.6.1.4.1.12902.1.1.3.2.4.0
DHCPD	DHCPD service down	.1.3.6.1.4.1.12902.1.1.3.2.5.0
HTTPD	Web service down	.1.3.6.1.4.1.12902.1.1.3.2.6.0
ANTMGR	Antmgr service down	.1.3.6.1.4.1.12902.1.1.3.2.7.0
NAMED	DNS service down	.1.3.6.1.4.1.12902.1.1.3.2.8.0
ANT_HEARTBEAT	Heartbeat service down	.1.3.6.1.4.1.12902.1.1.3.2.9.0
SIPLOGIN	SIP login service down	.1.3.6.1.4.1.12902.1.1.3.2.10.0
DNSREDIR	DNS redirector down	.1.3.6.1.4.1.12902.1.1.3.2.11.0
QMAIL	Qmail service down	.1.3.6.1.4.1.12902.1.1.3.2.12.0
SYSLOAD	System load too high	.1.3.6.1.4.1.12902.1.1.3.2.13.0

HTTPDUP	Web service restored	.1.3.6.1.4.1.12902.1.1.3.2.14.0
MYSQLDUP	Database service restored	.1.3.6.1.4.1.12902.1.1.3.2.15.0
SQUIDUP	Web proxy service restored	.1.3.6.1.4.1.12902.1.1.3.2.16.0
DHCPDUP	DHCPD service restored	.1.3.6.1.4.1.12902.1.1.3.2.17.0
NAMEDUP	DNS service restored	.1.3.6.1.4.1.12902.1.1.3.2.18.0
ARPDUP	ARPD service restored	.1.3.6.1.4.1.12902.1.1.3.2.19.0
ANTMGRUP	Antmgr service restored	.1.3.6.1.4.1.12902.1.1.3.2.20.0
DNSREDIRUP	DNS redirector restored	.1.3.6.1.4.1.12902.1.1.3.2.21.0
QMAILUP	Qmail service restored	.1.3.6.1.4.1.12902.1.1.3.2.22.0
SIPLOGINUP	SIP login service restored	.1.3.6.1.4.1.12902.1.1.3.2.23.0
PFMGR	Pfmgr service down	.1.3.6.1.4.1.12902.1.1.3.2.24.0
PFMGRUP	Pfmgr service restored	.1.3.6.1.4.1.12902.1.1.3.2.25.0
ANTHEARTBEATUP	Heartbeat service restored	.1.3.6.1.4.1.12902.1.1.3.2.26.0
DHCPDGETOMAPI	DHCPD failed to assign public IP address	.1.3.6.1.4.1.12902.1.1.3.2.27.0
DHCPDRELEASEOMAPI	DHCPD failed to release public IP address	.1.3.6.1.4.1.12902.1.1.3.2.28.0
ANT_HA PROMOTION TRAP	Server has just been promoted to master in a HA setup	.1.3.6.1.4.1.12902.1.1.1.3.1
ANT_HA DEMOTION TRAP	Server has just been demoted to slave in a HA setup	.1.3.6.1.4.1.12902.1.1.1.3.2
SNMPv2-MIB: coldStart	Sent whenever the SNMP agent starts up (due to process restart or server reboot, etc.)	.1.3.6.1.6.3.1.1.5.1
UCD-SNMP-MIB ucdShutdown	Sent whenever the SNMP agent terminates (due to process restart or server reboot, etc.)	.1.3.6.1.4.1.2021.251.2

The following are the service event SNMP traps sent by the InnGate:

Trap Ref	Description	OID
arpdUp	ARPD service restored	1.3.6.1.4.1.12902.1.1.4.2.1.1.1
arpdDown	ARPD service down	1.3.6.1.4.1.12902.1.1.4.2.1.1.2
mysqldUp	Database service restored	1.3.6.1.4.1.12902.1.1.4.2.1.2.1
mysqldDown	Database service down	1.3.6.1.4.1.12902.1.1.4.2.1.2.2
squidUp	Web proxy service restored	1.3.6.1.4.1.12902.1.1.4.2.1.3.1
squidDown	Web proxy service down	1.3.6.1.4.1.12902.1.1.4.2.1.3.2
dhcpdUp	DHCPD service restored	1.3.6.1.4.1.12902.1.1.4.2.1.4.1
dhcpdDown	DHCPD service down	1.3.6.1.4.1.12902.1.1.4.2.1.4.2
dhcpdGetPublicIpFail	DHCPD public IP	1.3.6.1.4.1.12902.1.1.4.2.1.4.3

	assignment failure	
dhcpdReleasePublicIpFail	DHCPD public IP release failure	1.3.6.1.4.1.12902.1.1.4.2.1.4.4
httpdUp	Web service restored	1.3.6.1.4.1.12902.1.1.4.2.1.5.1
httpdDown	Web service down	1.3.6.1.4.1.12902.1.1.4.2.1.5.2
antmgrUp	Antmgr service restored	1.3.6.1.4.1.12902.1.1.4.2.1.6.1
antmgrDown	Antmgr service down	1.3.6.1.4.1.12902.1.1.4.2.1.6.2
namedUp	DNS service restored	1.3.6.1.4.1.12902.1.1.4.2.1.7.1
namedDown	DNS service down	1.3.6.1.4.1.12902.1.1.4.2.1.7.2
antHeartbeatUp	ANT Heartbeat service restored	1.3.6.1.4.1.12902.1.1.4.2.1.8.1
antHeartbeatDown	ANT Heartbeat service down	1.3.6.1.4.1.12902.1.1.4.2.1.8.2
antHearbeatAllLeader	All high availability nodes in master mode for too long	1.3.6.1.4.1.12902.1.1.4.2.1.8.3
antHearbeatAllFollower	All high availability nodes in slave mode for too long	1.3.6.1.4.1.12902.1.1.4.2.1.8.4
antHeartbeatLoneFollower	Lone node in slave mode for too long	1.3.6.1.4.1.12902.1.1.4.2.1.8.5
antHeartbeatFailover	ANT Heartbeat failover	1.3.6.1.4.1.12902.1.1.4.2.1.8.6
siploginUp	SIP Login service restored	1.3.6.1.4.1.12902.1.1.4.2.1.9.1
siploginDown	SIP Login service down	1.3.6.1.4.1.12902.1.1.4.2.1.9.2
dnsredirUp	DNS Redirector service restored	1.3.6.1.4.1.12902.1.1.4.2.1.10.1
dnsredirDown	DNS Redirector service down	1.3.6.1.4.1.12902.1.1.4.2.1.10.2
qmailUp	Qmail service restored	1.3.6.1.4.1.12902.1.1.4.2.1.11.1
qmailDown	Qmail service down	1.3.6.1.4.1.12902.1.1.4.2.1.11.2
networkUp	All network links restored	1.3.6.1.4.1.12902.1.1.4.2.1.12.1
networkDownstreamDown	Downstream network link down	1.3.6.1.4.1.12902.1.1.4.2.1.12.2
networkUpstreamDown	Upstream network link down	1.3.6.1.4.1.12902.1.1.4.2.1.12.3
networkHADown	High availability network link down	1.3.6.1.4.1.12902.1.1.4.2.1.12.4
networkGatewayDown	Upstream gateway unreachable	1.3.6.1.4.1.12902.1.1.4.2.1.12.5
heartbeatUp	Heartbeat service restored	1.3.6.1.4.1.12902.1.1.4.2.1.13.1
heartbeatDown	Heartbeat service	1.3.6.1.4.1.12902.1.1.4.2.1.13.2

	down	
heartbeatFailover	Heartbeat failover	1.3.6.1.4.1.12902.1.1.4.2.1.13.3
heartbeatFailback	Heartbeat failback	1.3.6.1.4.1.12902.1.1.4.2.1.13.4
pfmgrUp	PFMGR service restored	1.3.6.1.4.1.12902.1.1.4.2.1.14.1
pfmgrDown	Pfmgr service down	1.3.6.1.4.1.12902.1.1.4.2.1.14.2

The following are the system event SNMP traps sent by the InnGate:

Trap Ref	Description	OID
loadNormal	System load returns to normal	1.3.6.1.4.1.12902.1.1.4.2.2.1.1
loadWarning	System load reaches critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.1.2
loadCritical	System load passes critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.1.3
memoryNormal	System memory usage returns to normal	1.3.6.1.4.1.12902.1.1.4.2.2.2.1
memoryWarning	System memory usage reaches critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.2.2
memoryCritical	System memory usage passes critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.2.3
diskNormal	System disk usage returns to normal	1.3.6.1.4.1.12902.1.1.4.2.2.3.1
diskWarning	System disk usage reaches critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.3.2
diskCritical	System disk usage passes critical limit	1.3.6.1.4.1.12902.1.1.4.2.2.3.3

The following are the security event SNMP traps sent by the InnGate:

Trap Ref	Description	OID
dnsredirDos	DNS Redirector denial of service	1.3.6.1.4.1.12902.1.1.4.2.3.1.1
arpdIpConflict	ARPD IP conflict	1.3.6.1.4.1.12902.1.1.4.2.3.2.1
arpdArpDos	ARPD ARP denial of service	1.3.6.1.4.1.12902.1.1.4.2.3.2.2
arpdGratuitousArpDos	ARPD gratuitous ARP denial of service	1.3.6.1.4.1.12902.1.1.4.2.3.2.3
squidHttpDos	Web proxy reached maximum concurrent HTTP connection limit	1.3.6.1.4.1.12902.1.1.4.2.3.3.1
squidNonHttpDos	Web proxy reached maximum concurrent non-HTTP connection limit	1.3.6.1.4.1.12902.1.1.4.2.3.3.2
qmailDos	Qmail reached maximum concurrent SMTP connection limit	1.3.6.1.4.1.12902.1.1.4.2.3.4.1

8.8.2 Supported MIBs

The MIBs supported by the InnGate are as follows:

1. MIB2 (RFC 1213)

2. HOST Resources (RFC 1514)

3. MIB for SNMPv2 (RFC 1450)

4. UCD Davis MIBS
   (OID 1.3.6.1.4.1) (.iso.org.dod.internet.private.enterprises)

5. ANT*labs* private MIBs:

   a. Number of detected clients
      OID 1.3.6.1.4.1.12902.1.1.2.1.1.1.0

      .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).antlabs(12902).ezxcess(1).ezxcessModules(1).clientInfoMIB(2).clientInfoObjects(1).clientInfo(1).detectedClientNum(1).0

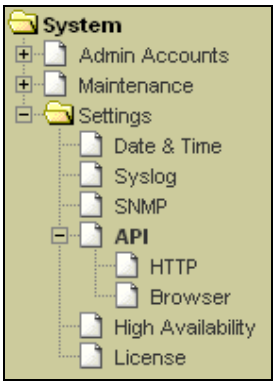
   b. Number of logged in clients
      OID 1.3.6.1.4.1.12902.1.1.2.1.1.2.0

      .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).antlabs(12902).ezxcess(1).ezxcessModules(1).clientInfoMIB(2).clientInfoObjects(1).clientInfo(1).internetClientNum(2).0

   c. Number of clients with Full Access
      OID 1.3.6.1.4.1.12902.1.1.2.1.1.3.0

      .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).antlabs(12902).ezxcess(1).ezxcessModules(1).clientInfoMIB(2).clientInfoObjects(1).clientInfo(1).payingClientNum(3).0

8.9 View API Information



To view the API information:

1. Click on **Settings**.
2. Click on **API**.

Figure 8-19 shows version information of the API and its modules installed in the InnGate.

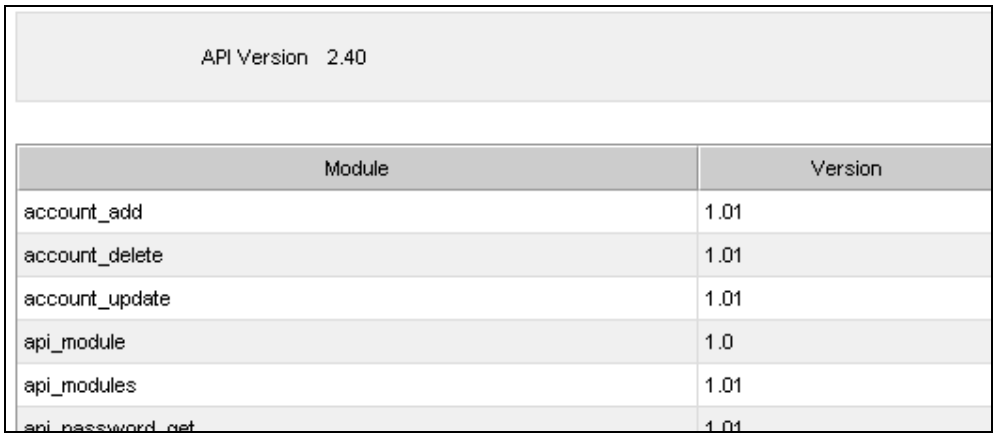
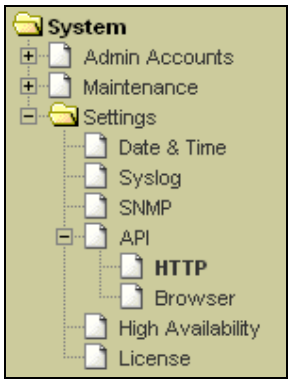


Figure 8-19 API Information

8.9.1 HTTP Setting

Configure the setting when making API calls via HTTP or HTTPS from downstream.



To view the configure HTTP setting:

1. Click on **Settings**.
2. Click on **API**.
3. Click on **HTTP**.

Figure 8-20 shows the settings to allow IP addresses to call API via HTTP or HTTPS.

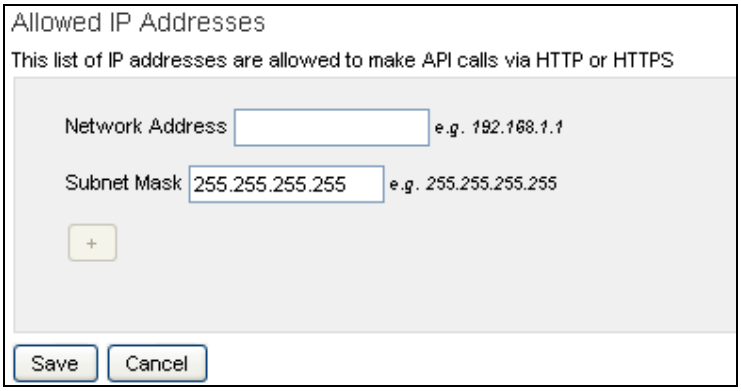


Figure 8-20 Allowed IP Addresses Setting

Click Save to confirm the changes.

Figure 8-21 shows the settings to change the API's password which is required when API is called via HTTP or HTTPS.

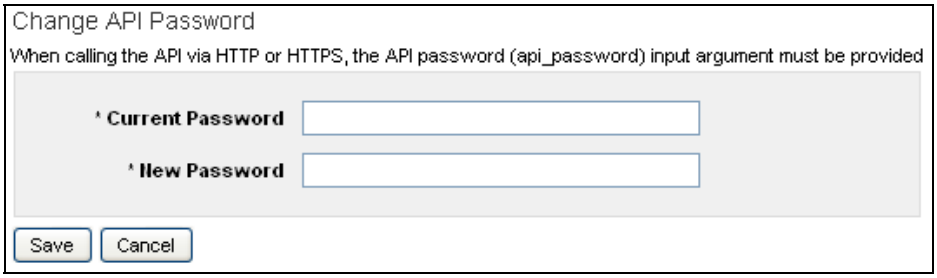
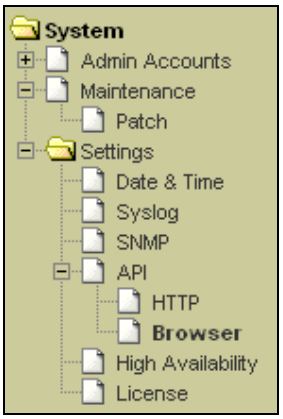

Change API Password
When calling the API via HTTP or HTTPS, the API password (api_password) input argument must be provided
* Current Password
* New Password
Save
Cancel

Figure 8-21 Change API Password Setting

Click Save to confirm the changes.

8.9.2 Browser Setting

Configure the matching user agent strings for PDA and phone browsers. This is used by the BrowserType() PHP API function and the "browser" API module to detect and return the browser type.



To view the configure Browser setting:

1. Click on **Settings**.
2. Click on **API**.
3. Click on **Browser**.

Figure 8-22 shows the existing configuration for browser setting.

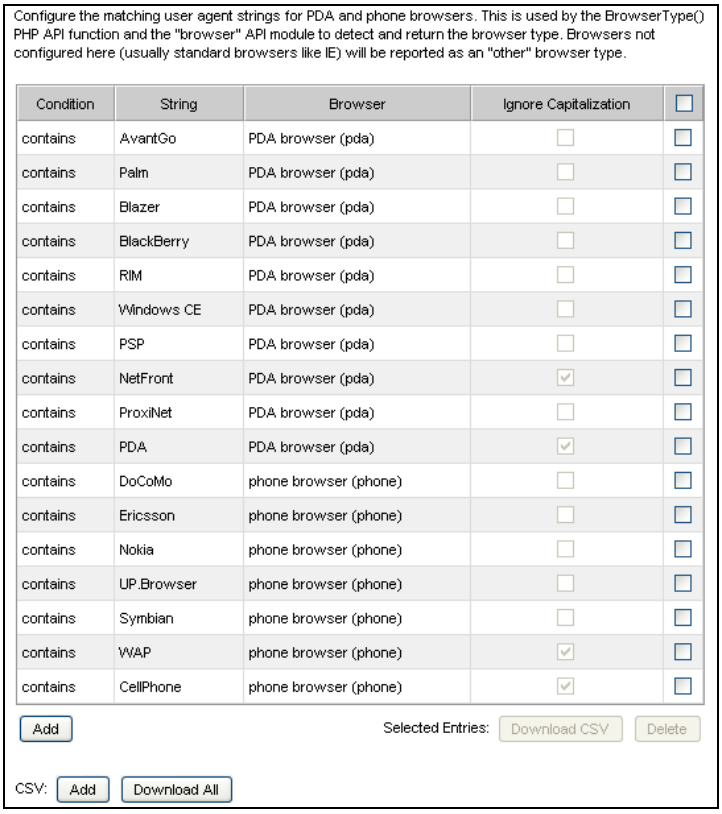

Configure the matching user agent strings for PDA and phone browsers. This is used by the BrowserType() PHP API function and the "browser" API module to detect and return the browser type. Browsers not configured here (usually standard browsers like IE) will be reported as an "other" browser type.
Condition String Browser Ignore Capitalization
contains AvantGo PDA browser (pda)
contains Palm PDA browser (pda)
contains Blazer PDA browser (pda)
contains BlackBerry PDA browser (pda)
contains RIM PDA browser (pda)
contains Windows CE PDA browser (pda)
contains PSP PDA browser (pda)
contains NetFront PDA browser (pda)
contains ProxiNet PDA browser (pda)
contains PDA PDA browser (pda)
contains DoCoMo phone browser (phone)
contains Ericsson phone browser (phone)
contains Nokia phone browser (phone)
contains UP.Browser phone browser (phone)
contains Symbian phone browser (phone)
contains WAP phone browser (phone)
contains CellPhone phone browser (phone)
Add
Selected Entries:
Download CSV
Delete
CSV:
Add
Download All

Figure 8-22 API Browser Setting

Click button Add to add new configuration record.

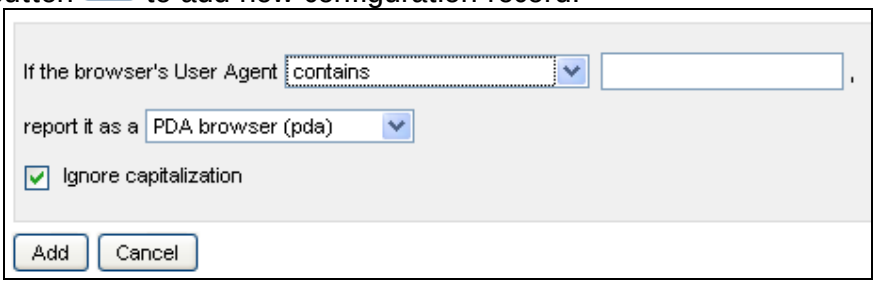


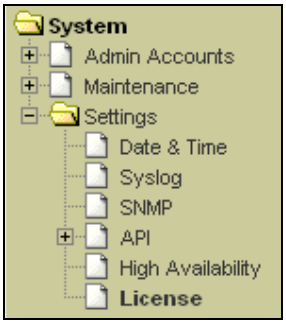
Figure 8-23 Adding New API Browser Setting

Click button Add to add the configuration.

8.10 High Availability

High Availability is explained in details in Chapter 9 and Chapter 10.

8.11 View License Information



To view the license information:

1. Click on **Settings**.
2. Click on **License**.

Figure 8-24 shows information regarding the number of devices that the InnGate is licensed to operate.

⚠ The **Serial Number** pertains to the licensing serial number and is not the same as the hardware serial number found on the equipment.

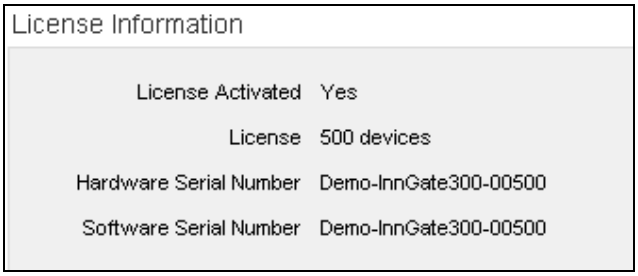


Figure 8-24 License Information

8.12 Console Access via Serial Connection

You can access the InnGate in console mode via a direct serial connection. Once connected and logged in, you will be presented with the command line interface (CLI) just like a Telnet session.

⚠ This list of commands is separately documented in the **Command Line Interface Reference**. Most of the CLI commands accessible via the Console

are also accessible via Telnet. However, as a physical security measure, some potentially destructive commands can only be executed via the Console.

To connect to the InnGate Console:

1. Connect the serial cable from your PC to the Serial Port of the InnGate.

2. Use your PC's terminal software to open an SSH session to the InnGate with the following terminal settings:

    a. Baud rate – 115200
    b. Data bits – 8
    c. Parity – None
    d. Stop bits – 1
    e. Flow Control – None

The default login ID and password is the same as for Telnet access and was previously discussed in Section 5.5.1.

8.13 Securing the System for Deployment

Once the InnGate has been configured and deployed, for security reasons, it is recommended that you:

1. **Securing Access** to the Admin GUI – See Section 8.13.1.

2. **Change the Default Admin User Account** – See Section 8.13.2.

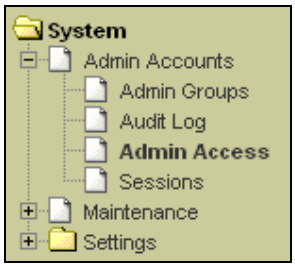
3. **Change the FTP Account Password** – See Section 8.13.3.

4. **Change the Telnet and Console Password** – See Section 8.13.4.

8.13.1 Securing Access to the Admin GUI

You can limit access to the web admin system by IP addresses and also block admin access from the downstream totally.

Do be extremely careful with this feature as you can potentially lock yourself out of the system! In the event that this happens, you will need to access the InnGate via serial console (see Section 8.12) and use a terminal-based software to shell into the InnGate to clear the lockout with this command: "`wadacc disable ip_control`" (please refer to **Command Line Interface Reference** documentation for more information on the `wadacc` command).



To configure the admin access:

1. Click on **Admin Accounts**.
2. Click on **Admin Access**.

Figure 8-25 shows the interface for configuring the admin access settings:

1. **Deny users from accessing this Admin system via LAN** – If enabled, access to the Admin GUI from the downstream is prohibited.
2. **Limit users accessing this admin system to these IP Addresses / Subnet Mask pairs** – If enabled, only client machines whose IP addresses are listed here will be allowed to access the Admin GUI (from the upstream).

   Click [+] and [-] to add and remove the IP address and subnet mask entries defined.

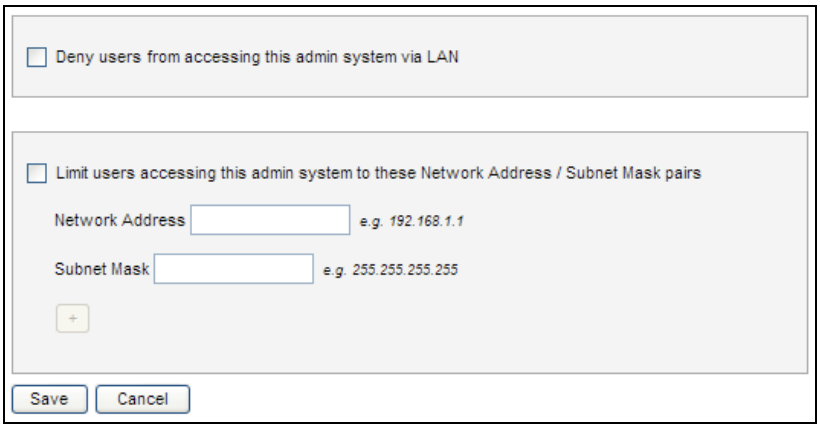
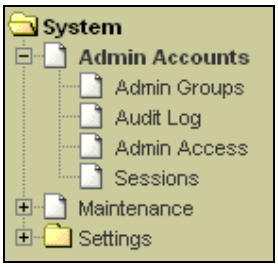

Deny users from accessing this admin system via LAN
Limit users accessing this admin system to these Network Address / Subnet Mask pairs
Network Address
e.g. 192.168.1.1
Subnet Mask
e.g. 255.255.255.255
Save
Cancel

Figure 8-25 Admin Access Settings

Click [Save] to confirm the changes.

8.13.2 Change the Default Admin User Account



To modify the default admin user acoount:

1. Click on **Admin Accounts**.

2.

Any existing entries will be displayed (see Figure 8-5).

The default admin account goes by the name of "System Administrator". Click on the entry to proceed and change the User ID and Password.

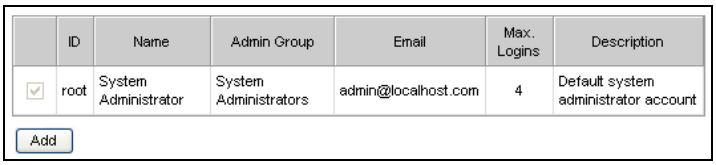


Figure 8-26 List of Administrator Accounts

8.13.3 Change the FTP Account Password

You can change the FTP account password through the CLI command **passwd_ftp**. First connect to the InnGate via Telnet (see Section 5.5.1) or Console (see Section 8.12). Then type in the command **passwd_ftp** as shown in Figure 8-27.

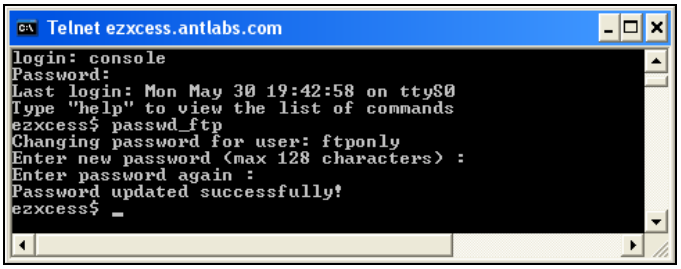


Figure 8-27 Change of FTP password

You will be prompted to key in your new password twice. If they match, your password will be updated successfully.

8.13.4 Change the Telnet and Console Password

The Telnet and Console user account is the same and changing the password will affect both Telnet and Console access. To change the password, logon to the InnGate via Telnet or Console and type the CLI command **passwd** as shown in Figure 8-28.

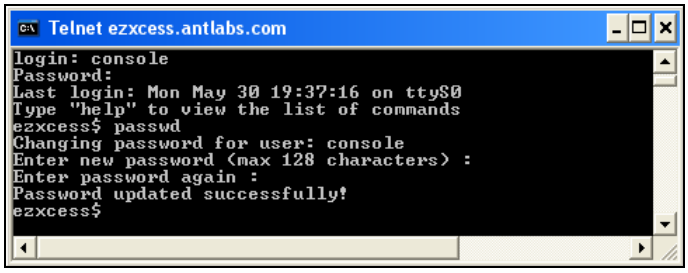


Figure 8-28 Change of Telnet/Console Password

Chapter 9

HIGH AVAILABILITY (E-Series)

9.1 Overview

The InnGate features high availability (HA) failover support capabilities to ensure continued operations in the event of a systems failure. The high availability feature couples two InnGate together with one operating in an active (Live InnGate) mode and the other in passive (Backup InnGate) mode. When a failover event occurs, the Backup InnGate will take over the network management responsibilities while the original Live InnGate attempts to recover.

This chapter describes the network setup requirements, GUI configurations and discusses the failover process.

9.2 Network Configuration

The network diagram in Figure 9-1 illustrates the basic connections for a typical HA setup in terms of the network connections.

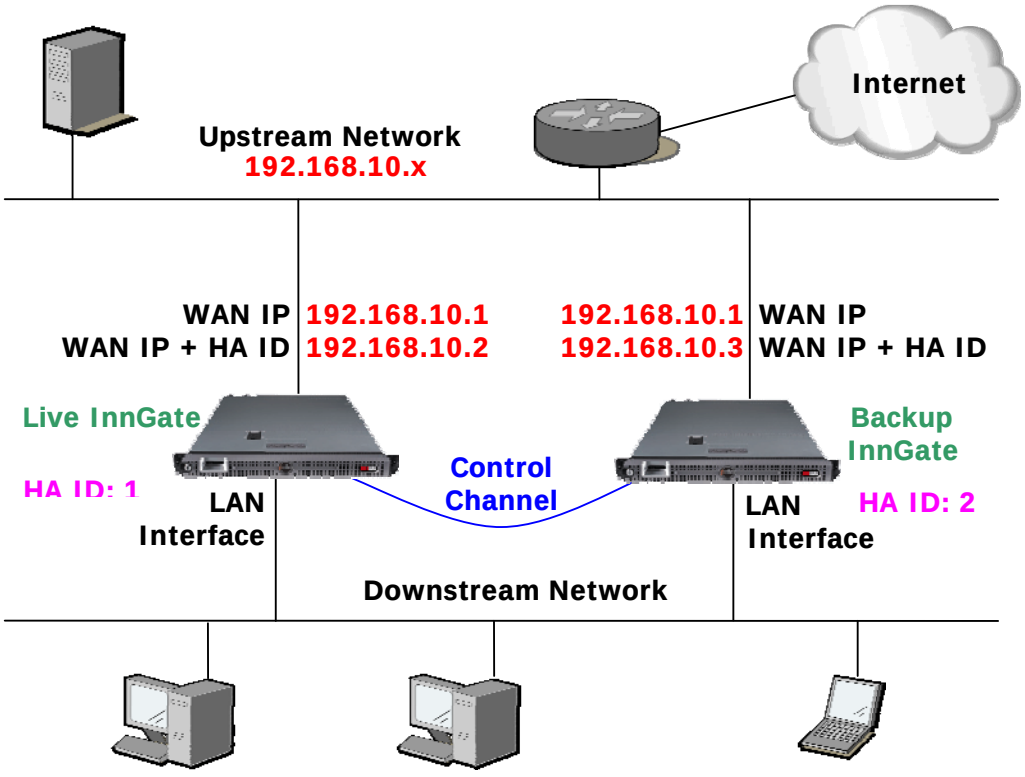


Figure 9-1 High Availability Setup

The key points to note when setting up the network for HA operations is summarized follows:

1. Both the Live and Backup InnGate must be connected to the same upstream and downstream networks (overlapping) via their individual WAN and LAN interfaces respectively as shown in the diagram.

2. The two InnGate will communicate directly through their **OPT** network interfaces (see Section 1.1.1) via a cross-cable connection. This link is called the **Control Channel** and is used by the InnGate to detect the state of its peer (heartbeat) and for regular synchronization of system configurations.

3. The two InnGate will be setup with the same WAN IP address (shown as **192.168.10.1** in the diagram) in their WAN profiles (see Section 4.2).

   In addition, each HA InnGate will automatically use an **additional IP address** which is derived from numerically adding the HA ID to the WAN IP (see Figure 9-1). This facilitates upstream clients when they need to probe and access each InnGate individually (with Ping and Telnet).

   ⚠ A HA setup will thus **require 3 IP addresses**. The Admin GUI will still be accessible only via the WAN IP (if accessing from the upstream) and will always be the Admin GUI of the Live InnGate.

Some potential problems due to setup errors are also highlighted here:

1. If the downstream network is not overlapping (due to configuration errors, switch failure, etc), the Backup InnGate will think that the Live InnGate is failing to service its downstream clients, triggering a failover event based on the behavior described in Section 9.5. This will keep repeating as the two InnGate continuously switch roles every time the failover occurs.

2. If the downstream network is not overlapping and the Control Channel also fails, then both InnGate may become active (Live InnGate). If we assume that the upstream network is overlapping, then they will cause a duplicate IP address problem on the network.

9.3 System Configuration

The steps involved to setup the HA implementation is as follows:

1. Bootup one of the InnGate. We will call this “InnGate Alpha”.

2. Make the necessary system configurations to InnGate Alpha.

3. Configure the HA settings (see Section 9.3.1).

4. Perform a system backup (optional).

5. Connect the upstream and downstream interfaces of InnGate Alpha to the network. Do not connect the Control Channel yet.

6. Shutdown InnGate Alpha. Changes will take effect when you next bootup.

7. Bootup the other InnGate. We will call this “InnGate Omega”.

8. Ensure the system configuration is identical to InnGate Alpha (e.g. WAN IP, DHCP, proxy, etc.)

9. Configure the HA settings (with a different identifier).

10. Shutdown InnGate Omega. Changes will take effect when you next bootup.

11. Bootup InnGate Alpha.

12. Connect the upstream and downstream interfaces of InnGate Alpha to the network and **connect the Control Channel** to InnGate Omega.

13. Ensure that InnGate Alpha operates correctly (e.g. downstream clients can login and access the Internet through the InnGate).

14. Bootup InnGate Omega. In accordance with the HA Leader Election Process (see Section 9.4), InnGate Alpha will become the Live InnGate and InnGate Omega will be the Backup InnGate.

15. Now when you login to the Admin GUI via the WAN IP address, you will be accessing the current Live InnGate (i.e. InnGate Alpha).

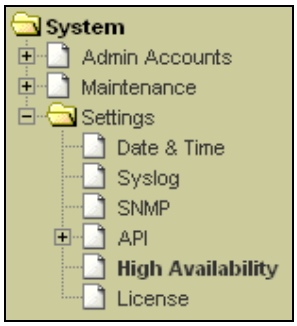
16. Perform a manual synchronization (see Section 9.6.1).

In a HA setup, attempting to login to the InnGate will always access the current Live InnGate. You can tell which physical machine this is by checking the HA identifier (see Section 9.3.1).

9.3.1 HA Identifier

Each of the InnGate in a HA setup is identified by a unique HA identifier which is used to differentiate the two gateways. This setting is configured in the Admin GUI.

⚠ The ID configured for each machine must be different otherwise the GUI synchronization, peer detection and HA failover will not function properly.



To setup the HA identifier:

1. Click on **Settings**.
2. Click on **High Availability**.

Figure 9-2 shows the interface for configuring the HA identifier:

1. **Slave Connected**: Indicates if a slave machine is connected to the machine.
2. **ID for This Unit** – The HA ID for this machine (permissible values are either 1 or 2).

   ⚠ The ID is only used to uniquely distinguish the machines and does not represent whether the InnGate is the Live or Backup machine.

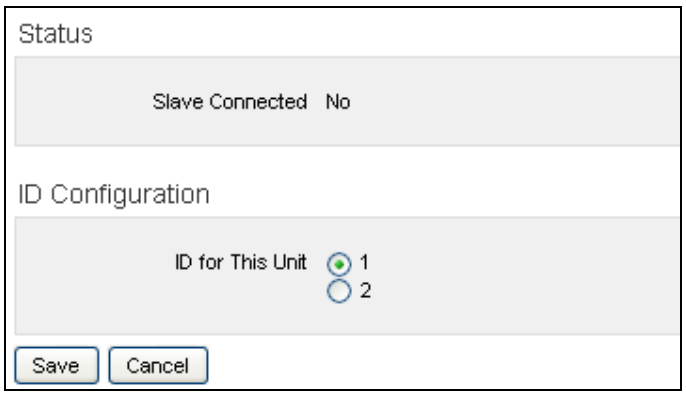


Figure 9-2 High Availability Configuration

Click Save to confirm the changes.

9.4 HA Leader Election

Whenever one of the InnGate in a HA setup boots up, it will attempt to determine whether it should assume the role of Live or Backup InnGate. This process is called the HA Leader Election.

To do this, the rebooted InnGate will first attempt to detect its peer over the Control Channel when it starts up. There are 2 possible conditions:

1. **Peer cannot be detected** – The InnGate will go into active mode (Live InnGate) by default.

2. **Existing peer is detected** – The InnGate with the shorter "runtime elapsed since last reboot" will switch to passive mode (Backup InnGate), ensuring that the "longer serving" system will be the Live InnGate.

It is possible that an existing Live InnGate is already in operation but because of a faulty or disconnected Control Channel link, both InnGate will end up in active mode which is problematic for the downstream clients. Should the Control Channel link be reconnected subsequently, the Leader Election process described in condition 2 above applies.

9.5 HA Failover Behavior

After the Leader Election process is completed, the both InnGate will begin failure event monitoring. Should a failover event be triggered, the HA Failover mechanism applies the STONITH approach to attempt to recover the faulty machine. Failover triggers are different depending on whether it is a Live or Backup InnGate.

The failover triggers for the **Live InnGate** are described as follows:

1. **LAN or WAN link (of the Live InnGate) is down** – The Live InnGate will check if the Backup InnGate's LAN and WAN links are functioning. If so, a failover is triggered.

2. **Failure of internal system components (of the Live InnGate)** – The Live InnGate will attempt to restart the malfunctioning system service. If this fails to restore the component, a failover is triggered.

The failover triggers for the **Backup InnGate** are described as follows:

1. **Backup InnGate detects failure (of the Live InnGate) to respond to downstream clients**.

2. **Failure to detect HA Leader heartbeat (over control channel)**.

The behavior of the Backup InnGate is the same for these two triggers. The Backup InnGate will simulate a downstream client and probe the Live InnGate to elicit a response.

If the Live InnGate fails to respond, the Backup InnGate will request for HA Leadership from the Live InnGate over the Control Channel and attempt to reboot (STONITH) the Live InnGate. During this process, the Backup InnGate will beep continuously.

When leadership is no longer held by the Live InnGate, the Backup InnGate will switch to active mode and assume the role of (new) Live InnGate. Three audio beeps will be sounded.

The (new) Live InnGate will also assume the virtual MAC addresses[2] of the downstream and upstream network interfaces of the (previous) Live InnGate and continue servicing the downstream clients.

Once (previous) Live InnGate boots up again, it will assume the role of (new) Backup InnGate in accordance with the HA Leader Election process described in Section 9.4.

⚠ The state of the Control Channel link alone is not a trigger for failover, so if the Control Channel link goes down (e.g. network interface or cable failure) a failover is not triggered, although other services dependent on the link such as GUI and client state synchronization may cease to function.

9.6 HA Synchronization

⚠ HA Synchronization can only be performed if Full HA module is installed in the InnGate.

The HA system supports automated periodic synchronization of some of the InnGate configuration settings and client state information from the Live InnGate to the Backup InnGate via the Control Channel.

Whenever the Backup InnGate boots up, it will download the current system configuration from the Live InnGate and subsequently synchronize these settings along with the downstream client states from the Live InnGate at **two minute intervals**.

In the event of a failover, the Backup InnGate will switch to active mode and assume the role of (new) Live InnGate as described in Section 9.5. When this happens the following process is carried out:

[2] Virtual MAC addresses are part of the HA feature. The Live SG always uses the Virtual MAC addresses while the Backup SG uses its own actual MAC addresses. Virtual MAC addresses enable a seamless failover as the rest of the network will always receive packets with the same MAC addresses.

1. The (new) Live InnGate will use the latest synchronized system configuration settings.

2. The (new) Live InnGate will assume the latest synchronized downstream client state as its current runtime state so that network operations can continue.

The following is a list of items that are **not** synchronized:

1. **Login volume accounting information** – This information cannot be recovered in the event of a failover. However, end-user login status, usage time, etc are recoverable.

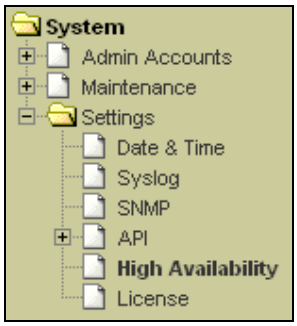
2. **FTP accessible system logs (email, web access, login logs)**

3. **Web patches** – System patches must be applied individually to both InnGate in a HA setup. You cannot just apply a patch to the Live InnGate and expect the synchronization process to copy the system image over to the Backup InnGate to produce a patched Backup InnGate.

9.6.1 Manual Synchronization

HA Manual Synchronization can only be performed if Full HA module is installed in the InnGate.

You may also perform a manual synchronization. This is often done as part of the initial HA setup process.



To perform a manual sync:

1. Click on **Settings**.

2. Click on **High Availability**.

Figure 9-3 shows the interface for invoking a manual synchronization.

Click Synchronize to begin the synchronization.

As the synchronization process may take a while, you can click Get Status to check on the progress.

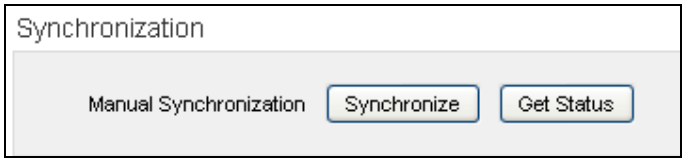


Figure 9-3 Manual Synchronization

Once completed, you will be presented with a log report of the synchronization process.

Chapter 10

HIGH AVAILABILITY (M-Series)

10.1 Overview

InnGate features high availability (HA) failover support to allow a secondary InnGate to be installed along with an existing primary InnGate to ensure that services continue to be provisioned in the event of a single system failure.

When a failover occurs, the secondary InnGate will change from **standby** mode to **active** mode and take over the network management responsibilities from the primary InnGate while the primary InnGate is recovered.

This chapter describes the network setup requirements, admin configuration and the failover process.

10.2 Network Configuration

The network diagram in Figure 10-1 shows the network connections needed for a typical HA setup.

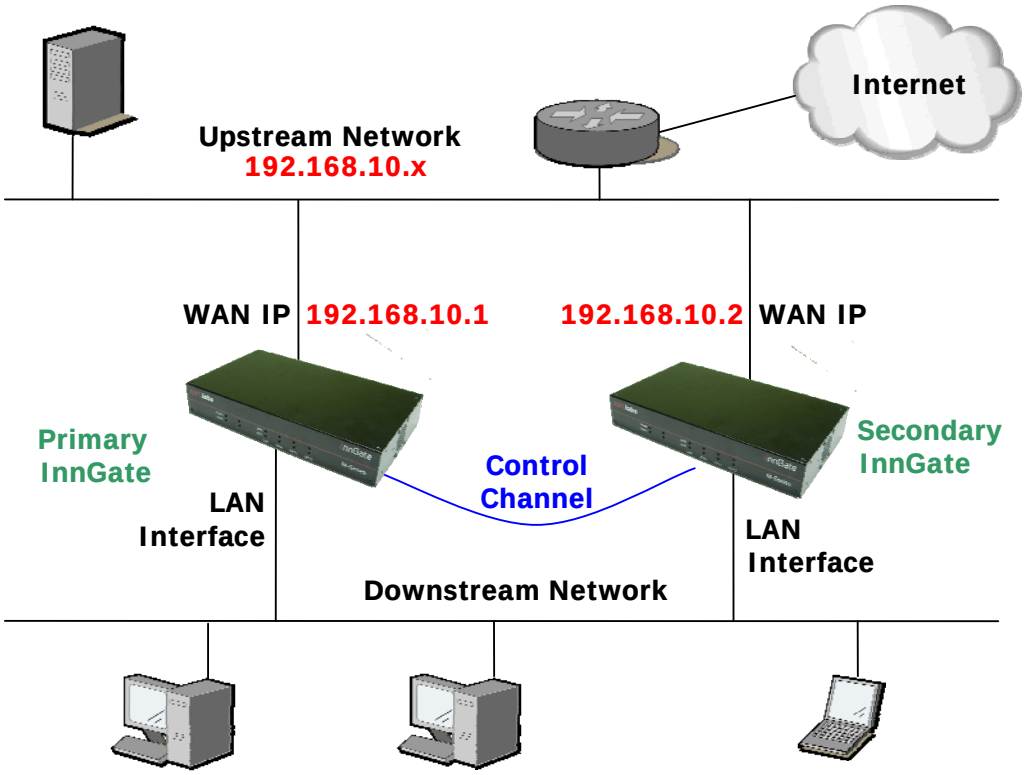


Figure 10-1 High Availability Setup

Both the primary and secondary InnGate requires:

1. An internet-accessible IP address each, assigned to the WAN interface. The WAN network and default gateways for both InnGates can be through the same link, or separate links for improved redundancy. (If it is through the same link, be careful not to assign the same IP address to both InnGates as this will cause a duplicate IP address problem on the network.)

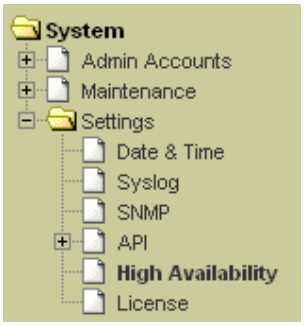
2. An Ethernet cross cable or dedicated switch connected to the OPT network interface to allow both gateways to communicate via a **control channel** link. This link is used by the primary and secondary InnGates to detect the state of its peer and trigger a failover when necessary.

3. A connection to the same downstream network and trunk VLANs via the LAN interface so that both InnGates can serve the same clients on the network.

⚠ The web admin of each InnGate can be accessed by the IP configured for the respective WAN port.

10.3 System Configuration

InnGates are factory-configured as primary gateways. They can be configured as the primary or secondary gateway in the admin GUI, as shown in Figure 10-2.



To configure HA:

1. Click on **Settings**.

2. Click on **High Availability**.

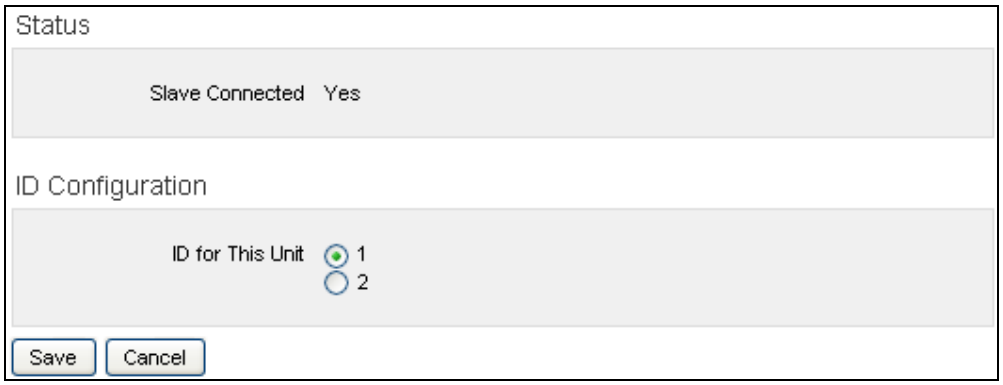


Figure 10-2 High Availability Configuration

Set the gateway as primary or secondary, and click Save to commit the changes. Reboot the gateway for the setting to take effect.

After changing InnGate from primary to secondary, do not connect to the LAN network until it is rebooted.

The configuration, policies and patches applied to both InnGates should be the same, so that when a failover occurs, network services are similarly provisioned.

The recommended steps to set up a HA deployment is as follows:

1. Start up the primary InnGate
2. Make the necessary system configuration changes
3. Set it as a primary InnGate
4. Reboot the primary InnGate for the HA settings to take effect
5. Connect the primary InnGate's WAN and LAN interfaces to the upstream and downstream networks
6. Start up the secondary InnGate
7. Configure the secondary InnGate with the same policies as the primary InnGate to ensure that it is correctly set up to take over in event of a HA failover
8. Set it as a secondary InnGate
9. Shut down the secondary InnGate

10. Connect the secondary InnGate's WAN and LAN interfaces to the upstream and downstream networks

11. Connect the primary and secondary InnGates via the OPT interface for the control channel link

12. Power on the secondary InnGate. The secondary InnGate will start up, discover the primary InnGate and set itself to standby.

⚠ The primary and secondary InnGates must be connected via the OPT interface so that they can see one another. This will prevent the secondary InnGate from becoming active after it boots up.

10.4 Billing Configuration

Additional care should be taken when configuring an InnGate that has billing enabled. This is to prevent situations where a failover occurs and users are billed again by the newly active InnGate because it does not know that billing was already done previously.

- Primary InnGate: Configured with billing plans
- Secondary InnGate: No billing policies, to prevent duplicate billing in the event of a failover

It is important that backups of the policies and web pages on the primary InnGate are made whenever they are changed.

If the primary InnGate has a downtime which exceeds the maximum billing duration of your billed usage plans, it is recommended to swap the primary and secondary roles of the InnGates such that the secondary InnGate will continue to serve the network as the primary gateway.

To do this:

1. Backup the policies and web pages of the secondary InnGate
2. Restore the primary InnGate's earlier backup to the secondary InnGate
3. Configure the secondary InnGate as the primary gateway

Once the primary InnGate is working again, it can be configured to work as the secondary gateway:

1. Restore the secondary InnGate's backup to the primary InnGate
2. Configure the primary InnGate as the secondary gateway

⚠ When policies are exchanged between both InnGates, it is important that the same patches have been applied to both gateways.

10.5 Failover Behavior

The primary InnGate will always be the active gateway unless one of the following occurs to trigger a failover to the secondary InnGate:

- WAN gateway is not responding to ARP pings
- InnGate is rebooting or shutting down

The secondary InnGate will failover and become active if any of the following occurs:

- Primary InnGate is not detected
- Control channel (OPT) link to the primary InnGate is down
- Received indication from the primary InnGate that it is rebooting or shutting down

A failback from the secondary InnGate to the primary InnGate will occur when the primary InnGate is:

- Turned on
- Detected again after a OPT link disconnection
- Able to contact its LAN and WAN networks again

If a valid email address is configured in System > Security > Admin Account, the secondary InnGate will send email notifications with the subject "High Availability Event Notification" whenever a failover or failback occurs.

Chapter 11

System Save & Restoration

11.1 Overview

InnGate 3 allows you to do 3 types of system save and restoration:

1. Save Snapshot
2. Restore Firmware
3. Restore Snapshot

11.2 Save Snapshot

Saving snapshot will save your current state configuration of the InnGate. This action can be performed through CLI in supervisor mode. To save snapshot through CLI:

1. Connect your PC or laptop to InnGate's USB Serial Console or Serial Console port using USB-Serial cable.
2. Open a Hyperterminal session. Login using *console* account (see Section 8.12).
3. Enable supervisor mode by typing *enasup*. No password is required.

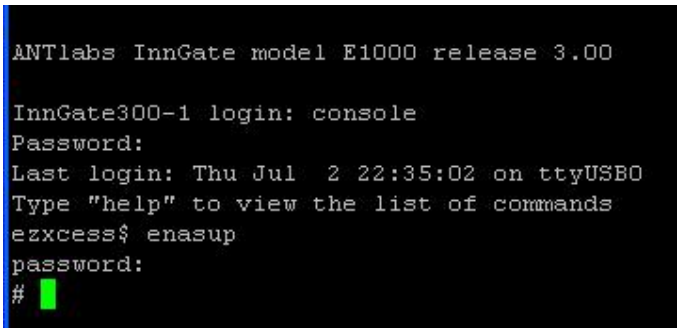


Figure 11-1 Enabling supervisor mode

4. Run the command by typing *save_snapshot*. There will be a prompt asking you whether you are sure to perform snapshot save. Press 'y' for yes or 'N' for cancel.

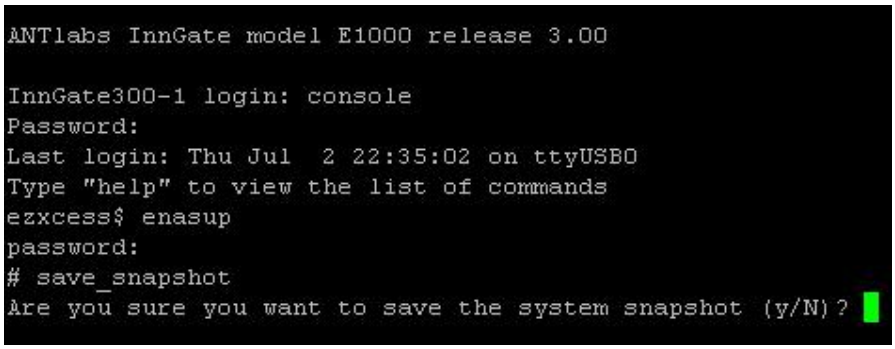

ANTlabs InnGate model E1000 release 3.00
InnGate300-1 login: console
Password:
Last login: Thu Jul 2 22:35:02 on ttyUSB0
Type "help" to view the list of commands
ezxcess$ enasup
password:
save_snapshot
Are you sure you want to save the system snapshot (y/N)?

Figure 11-2 Saving snapshot

Upon executing this command, the InnGate will reboot itself.

11.3 Restore Firmware

Restoring firmware will restore the InnGate to its factory default state. This action can be done through CLI in supervisor mode or through GRUB.

To restore firmware through CLI:

1. Connect your PC or laptop to InnGate's USB port using USB-serial cable.

2. Open a HyperTerminal session. Login using *console* account (see Section 8.12).

3. Enable supervisor mode by typing *enasup*. No password is required.

4. Run the command by typing *restore_snapshot*. There will be a prompt asking you whether you are sure to perform snapshot save. Press 'y' for yes or 'N' for cancel.

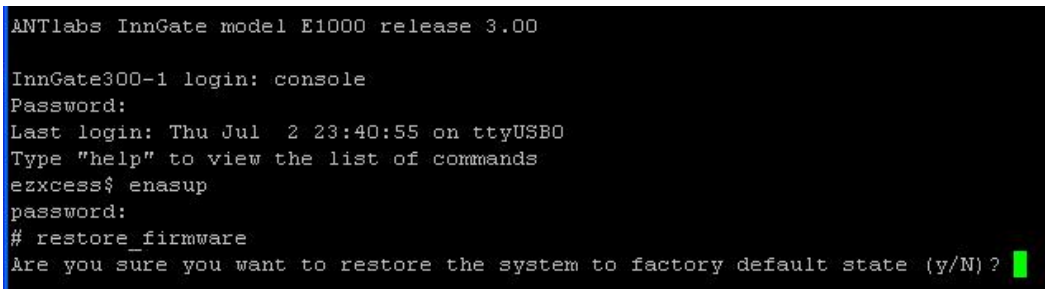

ANTlabs InnGate model E1000 release 3.00
InnGate300-1 login: console
Password:
Last login: Thu Jul 2 23:40:55 on ttyUSB0
Type "help" to view the list of commands
ezxcess$ enasup
password:
restore_firmware
Are you sure you want to restore the system to factory default state (y/N)?

Figure 11-3 Restoring Firmware

Upon executing this command, the InnGate will reboot itself to perform firmware restoration.

Once the firmware restoration has finished the IP address, subnet mask and default gateway will change into factory default setting. You need to change them appropriately and reboot the InnGate after you save the changes.

To restore through GRUB:

1. Connect your laptop or PC to the InnGate's PMS port using USB-serial cable.

2. Reboot the InnGate. Open a HyperTerminal session from your laptop or PC. Once the InnGate is up you should see as shown in Figure 11-4 below on your HyperTerminal window. Press ESC to skip memory test.

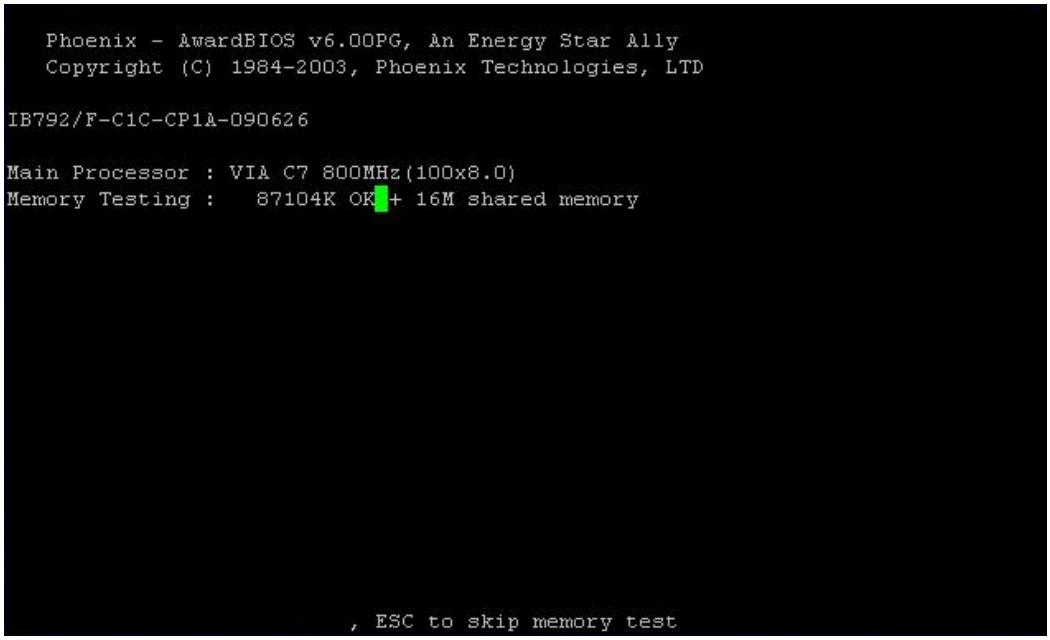

Phoenix - AwardBIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-2003, Phoenix Technologies, LTD
IB792/F-C1C-CP1A-090626
Main Processor : VIA C7 800MHz(100x8.0)
Memory Testing : 87104K OK + 16M shared memory
, ESC to skip memory test

Figure 11-4 Memory Test

3. After you see the system verifies DMI Pool Data on your screen, press any key to continue to GRUB selection menu.

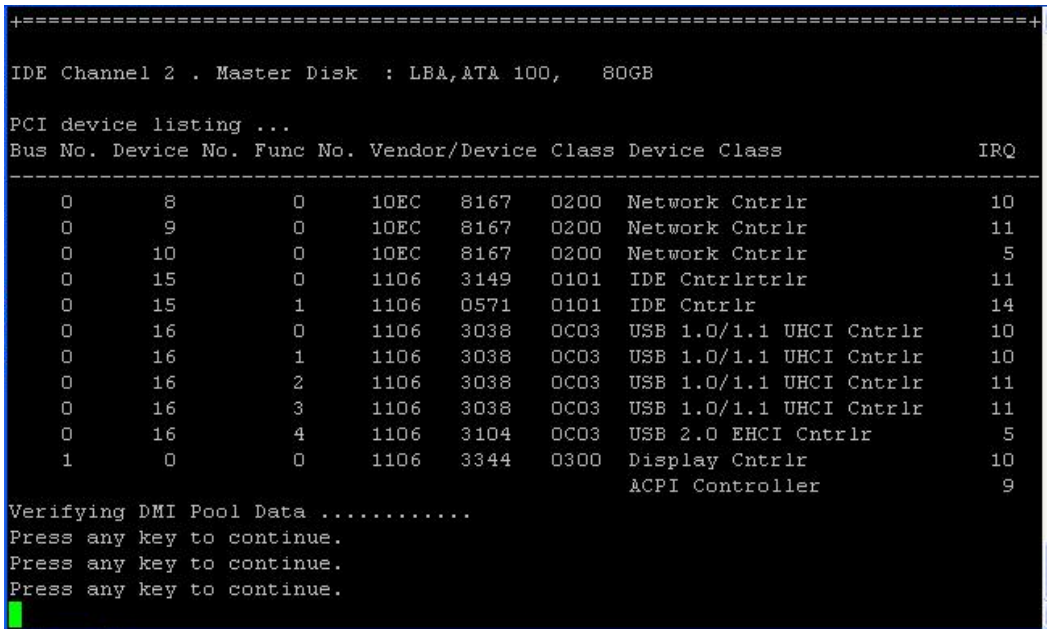

IDE Channel 2 . Master Disk : LBA,ATA 100, 80GB
PCI device listing ...
Bus No. Device No. Func No. Vendor/Device Class Device Class IRQ
0 8 0 10EC 8167 0200 Network Cntrlr 10
0 9 0 10EC 8167 0200 Network Cntrlr 11
0 10 0 10EC 8167 0200 Network Cntrlr 5
0 15 0 1106 3149 0101 IDE Cntrlrtrlr 11
0 15 1 1106 0571 0101 IDE Cntrlr 14
0 16 0 1106 3038 0C03 USB 1.0/1.1 UHCI Cntrlr 10
0 16 1 1106 3038 0C03 USB 1.0/1.1 UHCI Cntrlr 10
0 16 2 1106 3038 0C03 USB 1.0/1.1 UHCI Cntrlr 11
0 16 3 1106 3038 0C03 USB 1.0/1.1 UHCI Cntrlr 11
0 16 4 1106 3104 0C03 USB 2.0 EHCI Cntrlr 5
1 0 0 1106 3344 0300 Display Cntrlr 10
ACPI Controller 9
Verifying DMI Pool Data .....
Press any key to continue.
Press any key to continue.
Press any key to continue.

Figure 11-5 System verifies DMI Pool Data

4. You should see the GRUB selection menu as shown in Figure 11-6. Choose InnGate3.00 (Factory Firmware) to do firmware restoration.

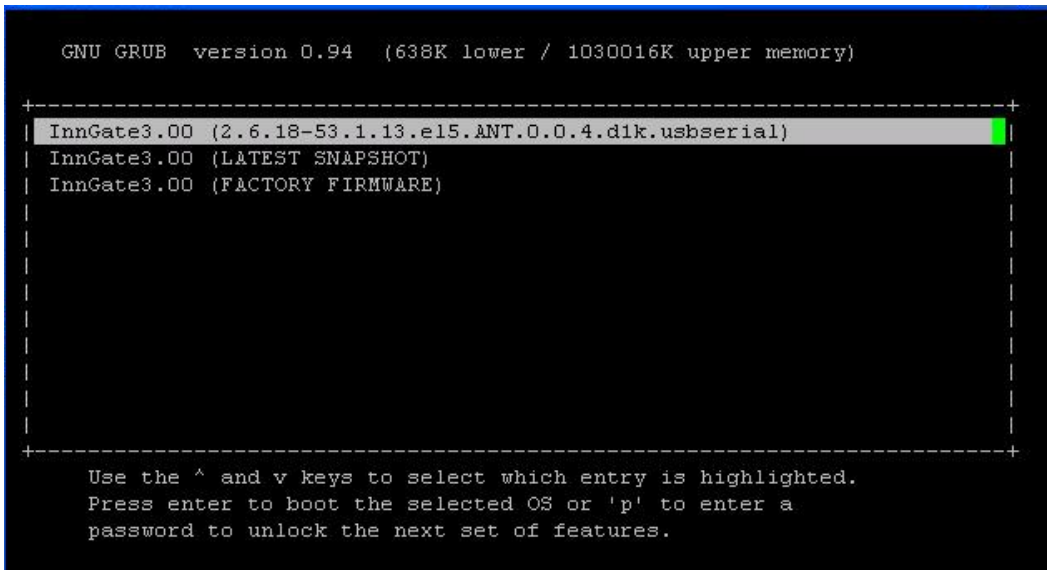

GNU GRUB version 0.94 (638K lower / 1030016K upper memory)
InnGate3.00 (2.6.18-53.1.13.el5.ANT.0.0.4.d1k.usbserial)
InnGate3.00 (LATEST SNAPSHOT)
InnGate3.00 (FACTORY FIRMWARE)
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.

Figure 11-6 GRUB Selection Menu

11.4 Restore Snapshot

Restoring snapshot will restore the InnGate to the latest saved state. This action can be done through CLI in supervisor mode.

To restore snapshot through CLI:

1. Connect your PC or laptop to InnGate's USB Serial Console or Serial Console port using USB-serial cable.

2. Open a HyperTerminal session. Login using *console* account (see Section 8.12).

3. Enable supervisor mode by typing *enasup*. No password is required.

4. Run the command by typing *restore_snapshot*. There will be a prompt asking you whether you are sure to perform snapshot save. Press 'y' for yes or 'N' for cancel.

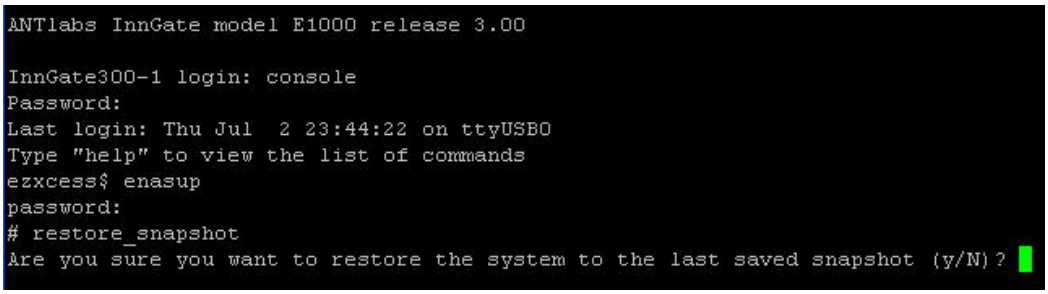

ANTlabs InnGate model E1000 release 3.00
InnGate300-1 login: console
Password:
Last login: Thu Jul 2 23:44:22 on ttyUSB0
Type "help" to view the list of commands
ezxcess$ enasup
password:
restore_snapshot
Are you sure you want to restore the system to the last saved snapshot (y/N)?

Figure 11-7 Restoring Snapshot

When there is no snapshot found, this action will be aborted.

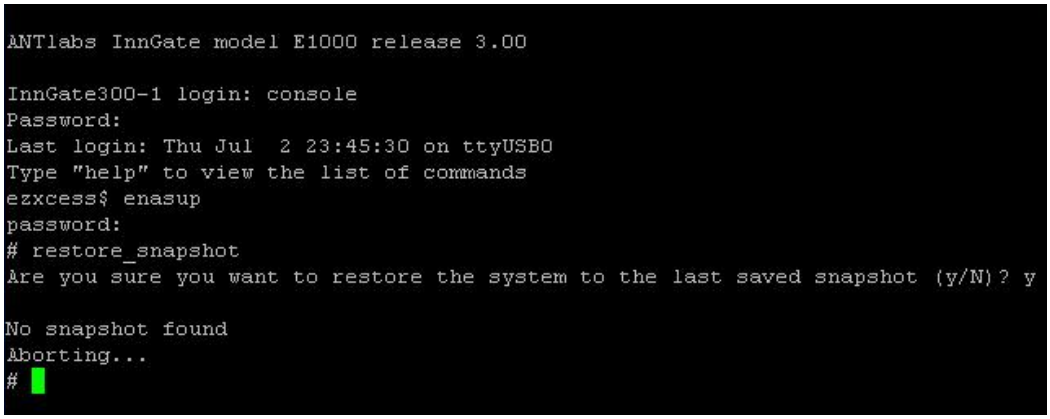

ANTlabs InnGate model E1000 release 3.00
InnGate300-1 login: console
Password:
Last login: Thu Jul 2 23:45:30 on ttyUSB0
Type "help" to view the list of commands
ezxcess$ enasup
password:
restore_snapshot
Are you sure you want to restore the system to the last saved snapshot (y/N)? y
No snapshot found
Aborting...
#

Figure 11-8 Aborting snapshot restore

Restoring snapshot through GRUB has the same steps as restoring firmware through GRUB. Refer to Section 11.3.

Appendix A

REDIRECT LOG

This is a sample of a redirect log showing the typical flow beginning with the user's first attempt to access the Internet (with accompanying explanations below each entry or set of entries). The redirect log is useful when diagnosing web access problems.

Each log entry consists of essentially 2 lines and follows the following format:

[Date/Time of entry**]** URL accessed User's IP address**/- -** HTTP Request type Destination IP address Interface number MAC address **Result(**Description**):** HTTP Response type**:**URL response sent to user

[Fri Jun 10 10:34:09 2005] http://www.google.com.sg/ 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(need_reg_defaulturl): 302:http://ezxcess.antlabs.com/www/pub/sample/singleclick-http.php

This is the user's first attempt at accessing the Internet. The user has just connected to the LAN and launched the Internet browser to access the URL http://www.google.com.sg/

The user's IP address is 10.128.0.1 and his browser has initiated a HTTP Get request to the destination IP address of 64.233.189.104 on port 80 (this is the DNS resolved IP address for http://www.google.com.sg/).

Other information such as the user's interface number (413) and MAC address (00:0E:35:7B:6D:D9) are also available.

Since the user has not logged in yet, the user is classified as unregistered and to be sent to the default URL (need_reg_defaulturl). The redirect is done with a HTTP 302 to the default URL http://ezxcess.antlabs.com/www/pub/sample/singleclick-http.php.

The singleclick-http.php is in fact the SingleClick login page.

[Fri Jun 10 10:34:09 2005] http://ezxcess.antlabs.com/www/pub/sample/singleclick-http.php 10.128.0.1/- - GET 192.168.123.50:80 413 00:11:D8:4C:2A:3B
Result(shopfront): http://127.0.0.1:80/www/pub/sample/singleclick-http.php

The user's browser is instructed to redirect to the singleclick-http.php and therefore makes a HTTP Get request for it.

The InnGate responds with the page http://127.0.0.1:80/www/pub/sample/singleclick-http.php. Notice that the IP address of the URL is 127.0.0.1 which indicates that the file resides on the InnGate. The Result description shopfront indicates that the user is surfing the pages prior to authentication.

[Fri Jun 10 10:34:12 2005] http://ezxcess.antlabs.com/login.now 10.128.0.1/- - POST 192.168.123.50:80 413 00:11:D8:4C:2A:3B
Result(shopfront):
http://127.0.0.1:80/api/?api_password=admin&op=auth_login&type=singleclick&client_mac=00:11:D8:4C:2A:3B&client_ip=10.128.0.1&location_index=3&ppli=eth0&successURL=http://ezxcess.antlabs.com/www/pub/sample/login-success.php?url=$requestedURL

The user enters clicks the "Go" button on the SingleClick login page. This action initiates a HTTP Post to login.now which resides on the InnGate (192.168.123.50:80).

The InnGate matches the Web Access SmartURL™ which invokes an API call for SingleClick login.

[Fri Jun 10 10:34:14 2005] http://ezxcess.antlabs.com/www/pub/sample/login-success.php?url=http%3A%2F%2Fwww.google.com.sg%2F 10.128.0.1/- - GET 192.168.123.50:80 413 00:11:D8:4C:2A:3B
Result(shopfront): http://127.0.0.1:80/www/pub/sample/login-success.php?url=http%3A%2F%2Fwww.google.com.sg%2F&client_mac=00:11:D8:4C:2A:3B

[Fri Jun 10 10:34:14 2005] http://ezxcess.antlabs.com/images/antlabs-logo.gif 10.128.0.1/- - GET 192.168.123.50:80 413 00:11:D8:4C:2A:3B
Result(shopfront): http://127.0.0.1:80/images/antlabs-logo.gif

These entries indicate a successful login and the login success page (including the associated images) is sent to the user. Notice that the initial URL that the user tried to access is also appended which can be used in the success page if desired. E.g. Auto-redirect.

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/ 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/images/hp0.gif 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/images/hp0.gif

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/images/hp1.gif 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/images/hp1.gif

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/images/hp2.gif 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/images/hp2.gif

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/images/hp3.gif 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/images/hp3.gif

[Thu Jun 10 10:34:22 2005] http://www.google.com.sg/favicon.ico 10.128.0.1/- - GET 64.233.189.104:80 413 00:11:D8:4C:2A:3B
Result(charged_internet): http://www.google.com.sg/favicon.ico

These entries indicate that the user has clicked on the link to re-attempt access to http://www.google.com.sg/. The domain name is resolved to 64.233.189.104 and the page is sent along with the associated images to the user's browser for display.

Appendix B

PERL REGULAR EXPRESSIONS

Some features in the InnGate allow you to specify regular expressions for input matching.

Here is an illustration of the application of regular expressions where you can use the "^" character to match the start of the URL.

Regular Expression: ^http://www.ezxcess.com	
Match:	**http://www.ezxcess.com**/mod?id=123
	http://www.ezxcess.com/index.html
Mismatch:	http://www.redirectaway.com?url=http://www.ezxcess.com

The InnGate recognizes Perl Regular Expressions and it is beyond the scope of this manual to discuss its full syntax. Instead, some references are provided:

1. http://www.perl.com/doc/manual/html/pod/perlre.html

2. http://www.perldoc.com/perl5.8.0/pod/perlre.html

Appendix C

CSV FILE RESTRICTIONS

When importing CSV file, the following points need to be taken note of:

1. The comma character (,) is the field separator. Thus if your text contains a comma, such as in a description, you must enclose that field with double quote characters as follows:

Text to be imported	**Field in CSV File**
Flower garden, Level 1	“Flower garden, Level 1”
Lounge access	Lounge access

2. Do not use the double quote character (") except to enclose strings in the manner described in point 1.

3. Do not use the single quote character (').

4. For multiple line input fields such as description fields, a new line (carriage return) is denoted by (\n) as follows:

Text to be imported	**Field in CSV File**
Flower garden Level 1	Flower garden\nLevel 1

Appendix D

UPLOADING CUSTOM WEBPAGES

To upload custom webpages:

1. Initiate an FTP session to the InnGate as shown in Figure D-1.

   See Section 5.5.1 for the default User ID and Password.

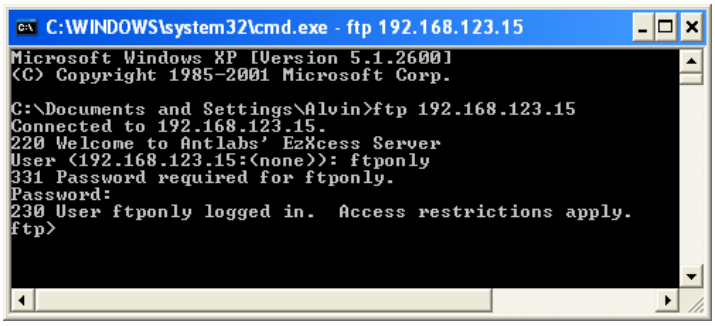

C:\WINDOWS\system32\cmd.exe - ftp 192.168.123.15
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Alvin>ftp 192.168.123.15
Connected to 192.168.123.15.
220 Welcome to Antlabs' EzXcess Server
User (192.168.123.15:(none)): ftponly
331 Password required for ftponly.
Password:
230 User ftponly logged in. Access restrictions apply.
ftp>

Figure D-1 Initiate an FTP session

2. Once logged in, you will be in the default webroot directory ("/"). This corresponds to the following webroot URL from the downstream:

   `http://ezxcess.antlabs.com/www/pub/`

3. Begin uploading your custom webpages.

   ⚠ You can only upload files and create new subdirectories in the "**login**" and "**ssl**" directories.

   For example, if you create a subdirectory "new" under the "login" directory and upload a webpage called "test.htm" there, the URL from the downstream to access the page will be:

   `http://ezxcess.antlabs.com/www/pub/login/new/test.htm`

Appendix E

CUSTOM SSL LOGIN PAGES

The InnGate supports HTTPS-based login using a custom SSL certificate. This section will give step-by-step instructions on how to enable secure HTTPS pages on the InnGate which is a 4 step process as follows:

1. Step 1 – Generate the Certificate Signing Request
2. Step 2 – Apply for a SSL Server Certificate
3. Step 3 – Install the Signed Certificate and Private Key
4. Step 4 – Configuring the HTTPS Login Page

⚠ The SSL Domain is only applicable on the downstream.

Step 1 – Generate the Certificate Signing Request

You can either generate the Certificate Signing Request (CSR) for the required domain using the ANT*labs* Cert Generator or by other means. Here we will describe how to do it with the ANT*labs* Cert Generator.

Firstly, obtain a copy of the ANT*labs* Cert Generator Windows program from your local ANT*labs* representative.

Next, run the installation program. When prompted to enter the password, key in "`antlabs`" as shown in Figure E-. Click on the **Next** button to continue with the installation.

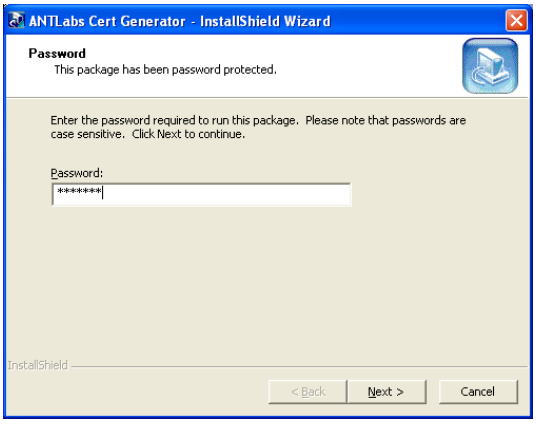

ANTLabs Cert Generator - InstallShield Wizard
Password
This package has been password protected.
Enter the password required to run this package. Please note that passwords are case sensitive. Click Next to continue.
Password:
InstallShield
< Back
Next >
Cancel

Figure E-1 Cert Generator Installation Password

Once the installation has completed, start the ANT*labs* Cert Generator application.

Fill in the CSR fields in the certificate generator interface as shown in Figure E-2.

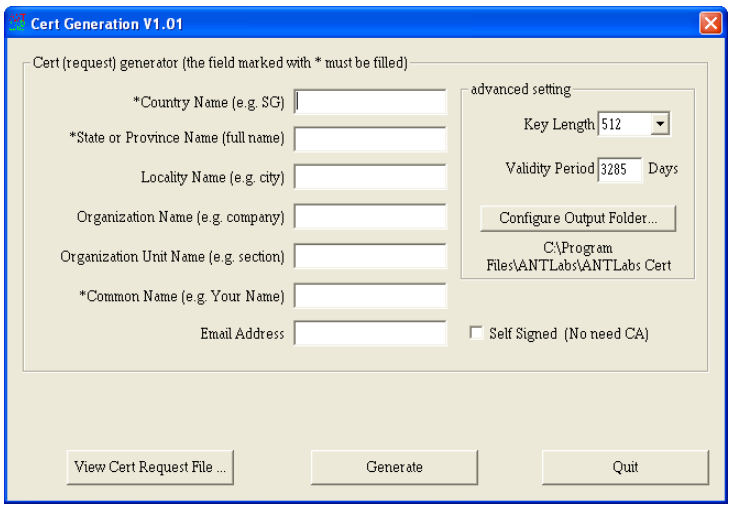


Figure E-2 Cert Generator Interface

Compulsory fields are marked with an asterisk " * " and are briefly described as follows:

1. **Country Name** – The two-letter ISO abbreviation for your country.

2. **State or Province Name** – The state or province where your organization is legally located. Cannot be abbreviated.

3. **Common Name** – This is the FQDN (Fully Qualified Domain Name) for which you plan to use your Certificate. For example, a certificate generated for antlabs.com will not be valid for secure.antlabs.com. If the web address to be used for SSL is secure.antlabs.com, ensure that the common name submitted in the CSR is secure.antlabs.com.

Click on the Generate button to generate the CSR and private key. If you want to generate a self-signed key, enable the "self signed" check box.

By default, the CSR and private key will be saved under the same installation directory as the software. You can change the default save folder by selecting the **Configure Output Folder...** button.

The CSR filename will be "<yourdomain>.csr". The private key filename will be "<yourdomain>.key".

Step 2 – Apply for a SSL Server Certificate

You need to apply for a SSL server certificate from a Certificate Authority (CA) by submitting the CSR you generated to a CA of your choice, e.g. Verisign, Thawte etc. Be careful not to submit your private key to the CA.

⚠ If you generated a self-signed certificate in the first step, you do not need to apply for a CA-signed certificate. However, your self-signed certificate will not be trusted by default.

Depending on the CA certificate application procedure, they may request for additional information.

Certification Information:

1. Web Server Type – Apache
2. CSR Format - PEM

⚠ You must own the domain for which you are applying the certificate.

Step 3 – Install the Signed Certificate and Private Key

Initiate an FTP session to the InnGate. See Section 5.5.1 for the default User ID and Password:

1. Change to the "`ssl`" directory and upload the signed certificate and private key.

   ⚠ The signed certificate filename extension must be "`crt`" (not "`csr`") and the private key filename extension must be "`key`". There must be only one "`.crt`" and matching one "`.key`" file in the "`ssl`" directory.

2. Reboot the InnGate.

To test the new certificate is working, make sure your web browser is configured not to use a web proxy (direct connection to the Internet) and from the service gateway downstream, access the new HTTPS URL Admin GUI, e.g. `https://<yourdomain>/admin/`. You should see the Admin GUI login page.

Step 4 – Configuring the HTTPS Login Page

This is only required if you want to display your login page via HTTPS. It is not necessary if you only want to secure the login User ID and Password information via HTTPS.

1. Ensure that the URL for the login page specified in your active Authentication Policy reflects "<yourdomain>" rather than the default "ezxcess.antlabs.com".

2. Modify the HTML code in the login page to post the login form to the new domain (i.e. "ezxcess.antlabs.com" to "<yourdomain>").

   Example,

   ```
   <form method="post" action="https://<yourdomain>/...
   ```

Appendix F

ERROR PAGES

You can create customized error page by putting a HTML or PHP file named with these names below to the "messages" FTP directory:

1. **blocked.ant –** This error page is shown when access is blocked by InnGate. When this file is not available InnGate will show the default error page below Figure F-1.

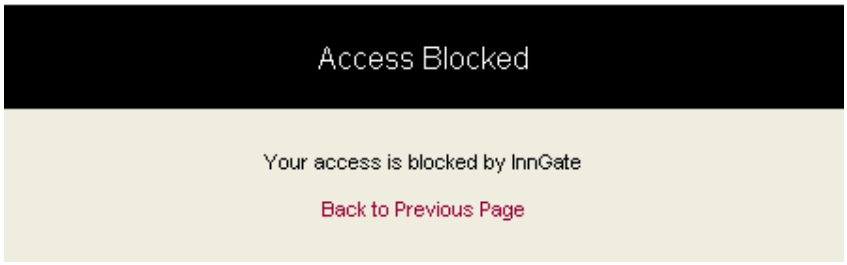


Figure F-1 Default blocked.ant

2. **location_config.ant –** This error page is shown when location has not been configured yet. When this file is not available InnGate will show the default error page below Figure F-2.

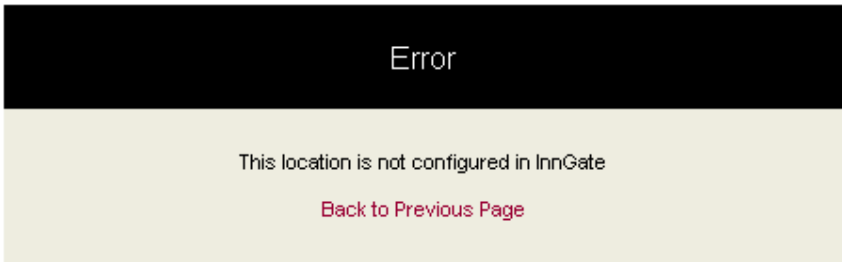


Figure F-2 Default location_config.ant

3. **config_error.ant –** This error page is shown when there is configuration error. When this file is not available InnGate will show the default error page as shown in Figure F-3.

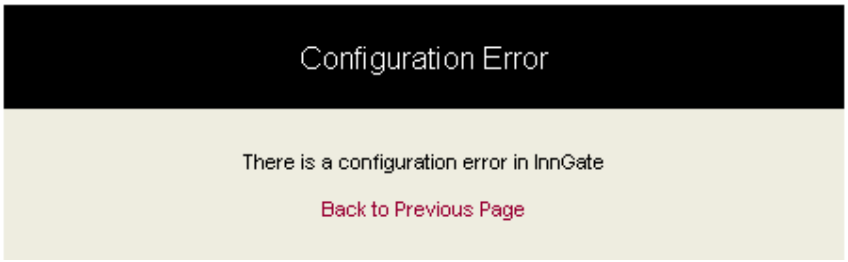


Figure F-3 Default config_error.ant

svc_failure.ant – This error page is shown when there is temporary service error. When this file is not available InnGate will show the default error page as shown in Figure F-4.

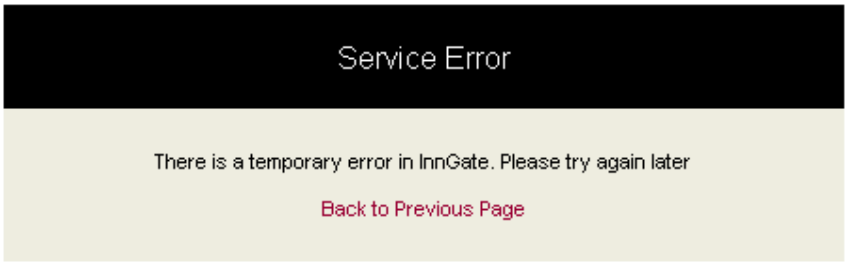


Figure F-4 Default svc_failure.ant

Appendix G

CREDIT CARD

Credit card payment gateways used by InnGate are:

1. **Worldpay Select Junior**

   Figure G-1 shows the Worldpay Select Junior's setting page.

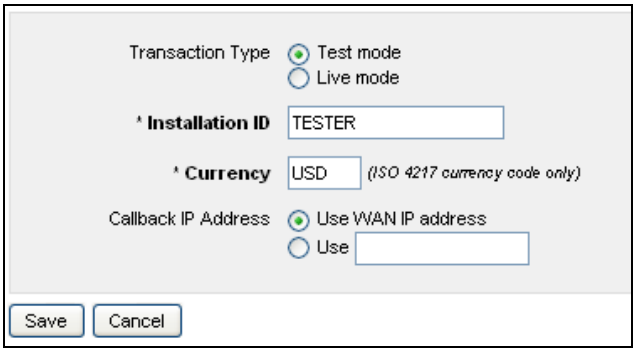


Figure G-1 Worldpay Select Junior Setting

   For details visit http://www.worldpay.com/.

2. **Paypal Payflow Pro**

   Figure G-2 shows the Paypal Payflow Pro's setting page.

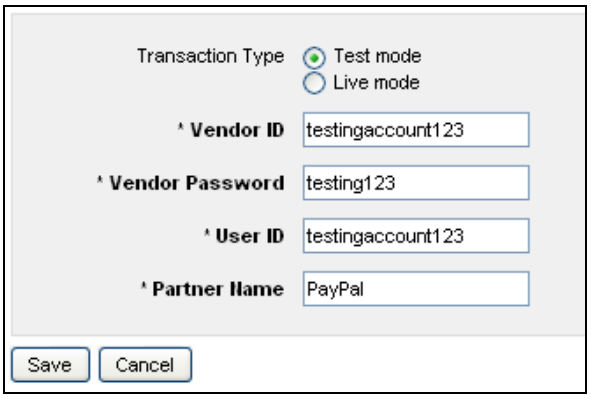


Figure G-2 Paypal Payflow Pro Setting

For details visit https://www.paypal.com/cgi-bin/webscr?cmd=_payflow-pro-overview-outside,

3. **Authorize.Net SIM**

Figure G-3 shows the Authorize.Net SIM's setting page.

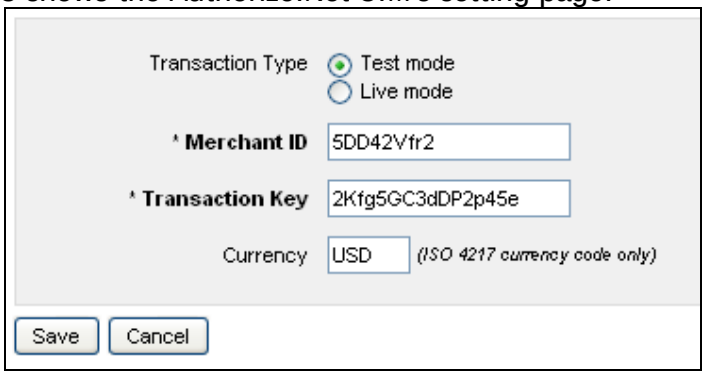


Figure G-3 Authorize.Net SIM Setting

For details visit http://www.authorize.net/

4. **Paypal Payflow Link**

Figure G-4 shows Paypal Payflow Link's setting page.

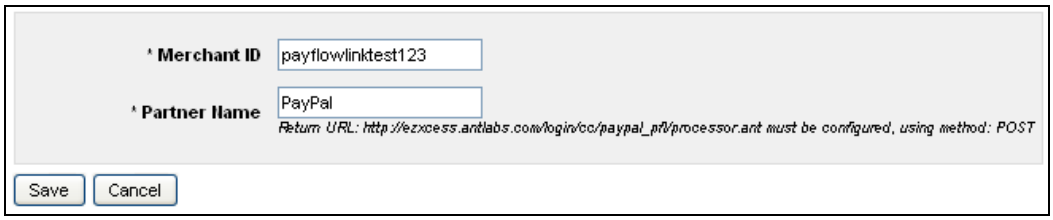


Figure G-4 Paypal Payflow Link Setting

For details visit https://www.paypal.com/cgi-bin/webscr?cmd=_payflow-link-overview-outside.

to the Admin GUI